

# **PERIODIC RESPONSE AND SPECTRAL ANALYSIS OF DIGITAL DATA SCRAMBLERS**

A Thesis Submitted  
In Partial Fulfilment of the Requirements  
for the Degree of  
**MASTER OF TECHNOLOGY**

by

**Flt. Lt. M. N. SREEDHAR**

to the

**DEPARTMENT OF ELECTRICAL ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR  
AUGUST, 1982**

23858

TO

AMMA

MARY

PARTHA

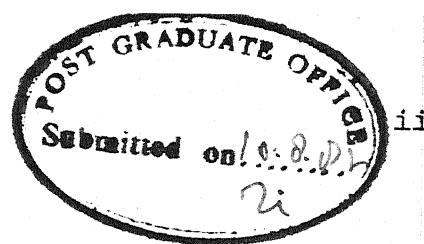
BUDDHIS

7 JUN 1984

CENTRAL LIBRARY

Ref. No. A 82862

EE-1982-M-SRE-PER



## CERTIFICATE

This is to certify that the work on PERIODIC RESPONSE AND SPECTRAL ANALYSIS OF DIGITAL DATA SCRAMBLERS has been carried out by Flt. Lt. M.N. Sreedhar under my supervision and has not been submitted elsewhere for a degree.

August 1982.

*M.U.Siddiqi*  
(M. U. Siddiqi)  
Assistant Professor  
Department of Electrical Engineering  
Indian Institute of Technology  
Kanpur.

ACKNOWLEDGEMENTS

I express my gratitude and respect to Dr. M.U. Siddiqi for his able guidance and encouragement during the complete period of this study.

I thank all the people who helped me in this work, be it a friend, a well-wisher, a relative or a casual associate.

I thank Mr. R.N. Srivastava and Mr. Tiwari for their excellent typing and cyclostyling of this thesis respectively.

Flt. Lt. M.N. Sreedhar

## CONTENTS

	Page
LIST OF TABLES	vii
LIST OF FIGURES	xi
ABSTRACT	xii
CHAPTER 1      INTRODUCTION	1
1.1      Spectrum of Periodic Data	2
1.2      Single Tone Interference	4
1.3      Adaptive Equalization	4
1.4      Spectrum of Received Signal	7
1.5      Timing Recovery from Zero Crossings	10
1.6      Precession and Its Effect on the Timing Recovery	13
1.7      Scrambler	18
1.8      Self Synchronizing Scramblers	19
1.9      Other Aspects of Scrambler Studies	24
1.9.3    Cascaded and Parallel Scramblers	25
1.9.4    Universal Scrambler	25
1.9.5    Systematic Jitter Suppression by Scrambling	26
1.9.6    Scrambler for Encryption	27
1.10     Scope of the Work	27
1.11     Organization of the Thesis	28
CHAPTER 2     MATHEMATICAL PRELIMINARY	31
2.1     Galois Field	31
2.2     Polynomials Over a Field	33
2.3     Construction of $GF(p^m)$	37
2.4     Partial Fraction Expansion of Polynomial	
	39

2.5	Partial Fraction Expansion of Polynomial Fraction Over Galois Fields	43
2.6	An Useful Result on Polynomials Over $GF(p)$	48
CHAPTER 3	SCRAMBLER ANALYSIS - INPUT OUTPUT RELATIONS	50
3.1	D-Transform	51
3.2	Representation of a Sequence by Polynomials	52
3.3	Periodicity of Two Periodic Sequences Added Bit by Bit	54
3.4	M-sequence Generator	55
3.5	Transfer Function of Scrambler	56
3.6	Output Period of Scrambler	57
3.7	Specific Illustrations	68
3.8	Complementary Partial Fraction Expansion	75
3.9	Critical State and Output of a Composite Sequence	80
CHAPTER 4	SPECTRAL THEORY OF LSC AND ITS APPLICATION TO SCRAMBLERS	85
4.1	Linear Sequential Circuits (LSC)	86
4.2	Total Response from Responser to Component Sequences	87
4.3	Basis Functions for the Vector Space of Periodic Galois Functions	89
4.4	Application to Scramblers	95
4.5	Fourier Series Expansion of Periodic Binary Sequences Over Finite Fields	103
4.6	Eigensignals and Eigenvalues of LSC	107
4.7	Application of Spectral Theory of Scramblers	111
4.7.1	Two Stage Scrambler	111
4.7.2	Three Stage Scrambler	125

4.7.3	Four Stage Scrambler	141
4.7.4	Five Stage Scrambler	149
CHAPTER 5	CONCLUSION	160
5.1	Conclusion	160
5.2	Suggestions for Further Research	161
REFERENCES		162
APPENDIX A	OPERATION TABLES FOR $GF(2^2)$ , $GF(2^3)$ , $GF(2^4)$ AND $GF(2^5)$	165
APPENDIX B	EIGENVALUES AND SPECTRAL COEFFICIENTS FOR VARIOUS STAGES OF SCRAMBLERS	169

## LIST OF TABLES

No.	Title	Page
1.1	Differential Encoding	17
1.2	Differential Encoding; Space Idle Condition	17
2.1	Addition and Multiplication Table for $GF(2)$	32
2.2	Addition and Multiplication Table for $GF(3)$	32
2.3	Addition and Multiplication Table for $GF(2^2)$	33
2.4	Addition and Multiplication Table for $GF(2^3)$	38
2.5	Addition and Multiplication Table for $GF(2^2)$	39
3.1	Zero Input Response and Their Transform; Example 3.3	65
3.2	Cases of Minimum Number of Transitions	74
3.3	Cases Where Scrambler Provides Delay for M-sequence	76
3.4	Table for Example 3.5	83
4.1	Spectral Coefficients at Input and Output for Sequences of Period 3; 2-stage Scrambler	114
4.2	Eigenvalues and Unique States in $GF(2^3)$ ; 2-stage Scrambler	116
4.3	Spectral Coefficients at Input and at Output for Sequences of Period 7; 2-stage Scrambler	117
4.4	Eigenvalue and Unique States in $GF(2^4)$ ; 2-stage Scrambler	119
4.5	Spectral Coefficients for Input and Output for Sequences of Period 5; 2-stage Scrambler	120
4.6	Spectral Coefficients at Input and Output for Sequences of Period 15; 2-stage Scrambler	123
4.7	Eigenvalues and Unique States in $GF(2^5)$ ; 2-stage Scrambler	126
4.8	Spectral Coefficients at Input and Output for Sequences of Period 31; 2-stage Scrambler	127

4.9	Eigenvalues and Unique States in $GF(2^2)$ ; $c(x) = x^3 + x + 1$	129
4.10	Spectral Coefficients at Input and Output for Sequences of Period 3; $c(x) = x^3 + x + 1$	130
4.11	Eigenvalues and Unique States in $GF(2^3)$ ; $c(x) = x^3 + x + 1$	130
4.12	Spectral Coefficients at Input and Output for Sequences of Period 7; $c(x) = x^3 + x + 1$	131
4.13	Eigenvalue and Unique States in $GF(2^4)$ ; $c(x) = x^3 + x + 1$	132
4.14	Spectral Coefficients at Input and Output for Sequences of Period 5; $c(x) = x^3 + x + 1$	133
4.15	Spectral Coefficients at Input and Output for Sequences of Period 15; $c(x) = x^3 + x + 1$	134
4.16	Eigenvalues and Unique States in $GF(2^5)$ ; $c(x) = x^3 + x + 1$	138
4.17	Spectral Coefficients at Input and Output for Sequences of Period 31; $c(x) = x^3 + x + 1$	139
4.18	Eigenvalues and Unique States in $GF(2^2)$ ; $c(x) = x^4 + x + 1$	142
4.19	Spectral Coefficients at Input and Output of Sequences of Period 7; $c(x) = x^4 + x + 1$	142
4.20	Eigensequences and Unique States in $GF(2^3)$ ; $c(x) = x^4 + x + 1$	144
4.21	Spectral Coefficients at Input and Output for Sequences of Period 7; $c(x) = x^4 + x + 1$	145
4.22	Eigenvalues and Unique States in $GF(2^4)$ ; $c(x) = x^4 + x + 1$	
4.23	Spectral Coefficients at Input and Output for Sequences of Period 5; $c(x) = x^4 + x + 1$	147
4.24	Spectral Coefficients at Input and Output for Sequences of Period 15; $c(x) = x^4 + x + 1$	148
4.25	Eigenvalues and Unique States in $GF(2^3)$ ; $c(x) = x^5 + x^2 + 1$	150
4.26	Spectral Coefficients at Input and Output for Sequences of Period 7; $c(x) = x^5 + x^2 + 1$	151

4.27	Eigenvalues and Unique States in $GF(2^4)$ ; $c(x) = x^5 + x^2 + 1$	153
4.28	Spectral Coefficients at Input and Output for Sequences of Period 15; $c(x) = x^5 + x^2 + 1$	154
4.29	Eigenvalues and Corresponding Unique States in $GF(2^5)$ ; $c(x) = x^5 + x^2 + 1$	156
4.30	Spectral Coefficients at Input and Output for Sequences of Period 31; $c(x) = x^5 + x^2 + 1$	157
A.1	Addition Table for $GF(2^2)$	165
A.2	Addition Table for $GF(2^3)$	166
A.3	Addition Table for $GF(2^4)$	167
A.4	Addition Table for $GF(2^5)$	168a
B.1	Eigenvalues and Unique States in $GF(2^3)$ ; $c(x) = x^3 + x^2 + 1$	169
B.2	Spectral Coefficients at Input and Output for Sequences of Period 7; $c(x) = x^3 + x^2 + 1$	169
B.3	Eigenvalues and Unique States in $GF(2^4)$ $c(x) = x^3 + x + 1$	170
B.4	Spectral Coefficients at Input and Output for Sequences of Period 15; $c(x) = x^3 + x^2 + 1$	171
B.5	Eigenvalues and Unique States in $GF(2^5)$ ; $c(x) = x^3 + x^2 + 1$	172
B.6	Spectral Coefficients at Input and Output for Sequence of Period 31; $c(x) = x^3 + x^2 + 1$	173
B.7	Eigenvalues and Unique States in $GF(2^5)$ ; $c(x) = x^4 + x + 1$	175
B.8	Spectral Coefficients at Input and Output for Sequence of Period 31; $c(x) = x^4 + x + 1$	176
B.9	Eigenvalues and Unique States in $GF(2^2)$ ; $c(x) = x^4 + x^3 + 1$	178
B.10	Spectral Coefficients at Input and Output for Sequences of Period 3; $c(x) = x^4 + x^3 + 1$	178
B.11	Eigenvalues and Unique States in $GF(2^3)$ ; $c(x) = x^4 + x^3 + 1$	179

B.12	Spectral Coefficients at Input and Output for Sequences of Period 7; $c(x) = x^4 + x^3 + 1$	179
B.13	Eigenvalues and Unique States in $GF(2^4)$ ; $c(x) = x^4 + x^3 + 1$	180
B.14	Spectral Coefficients at Input and Output for Sequences of Period 5; $c(x) = x^4 + x^3 + 1$	180
B.15	Spectral Coefficients at Input and Output for Sequences of Period 15; $c(x) = x^4 + x^3 + 1$	181
B.16	Eigenvalues and Unique States in $GF(2^5)$ ; $c(x) = x^4 + x^3 + 1$	182
B.17	Spectral Coefficients at Input and Output for Sequences of Period 31; $c(x) = x^4 + x^3 + 1$	183
B.18	Eigenvalues and Unique States in $GF(2^3)$ ; $c(x) = x^5 + x^4 + x^2 + x + 1$	185
B.19	Spectral Coefficients at Input and Output for Sequences of Period 7; $c(x) = x^5 + x^4 + x^2 + x + 1$	185
B.20	Eigenvalues and Unique States in $GF(2^4)$ ; $c(x) = x^5 + x^4 + x^2 + x + 1$	186
B.21	Spectral Coefficients at Input and Output for Sequences of Period 15; $c(x) = x^5 + x^4 + x^2 + x + 1$	187
B.22	Eigenvalues and Unique States in $GF(2^5)$ ; $c(x) = x^5 + x^4 + x^2 + x + 1$	188
B.23	Spectral Coefficients at Input and Output for Sequences of Period 31; $c(x) = x^5 + x^4 + x^2 + x + 1$	189

LIST OF FIGURES

No.	Title	Page
1.1	Gating Function	3
1.2	Spectrum of Gating Function	3
1.3	Data Stream ...1001...	3
1.4	Basic Group Modulation Scheme	5
1.5	Block Diagram of a Communication System	6
1.6	Block Diagram of a Communication System with Equalizer	6
1.7	Block Diagram of a Digital Transmission Scheme	7
1.8	Spectrum Given in Equation 1.15	9
1.9	Timing Recovery Scheme	11
1.10(a)	Spectrum without Precession	15
1.10(b)	Spectrum with Precession	15
1.11(a)	Spectrum without Precession	15
1.11(b)	Spectrum with Precession	15
1.12	DPSK Modulator	17
1.13	Block Diagram of a Communication System with Scrambler	18
1.14	A Scrambling Scheme	20
1.15(a)	Self Synchronising Scrambler	21
1.15(b)	Descrambler	21
1.16(a)	Universal Scrambler	26
1.16(b)	Descrambler	26
3.1	Addition of Two Sequences by Shift Registers	54
3.2	M-sequence Generator Structure	55
3.3	Scrambler; M-sequence Generator	56
3.4	Scrambler Structure	57

3.5	CACFs of Scrambled M-sequence	74b
4.1	Block Diagram of a LSC	86
4.2	Three Stage Scrambler; $c(x) = x^3 + x + 1$	95
4.3	Four Stage Scrambler; $c(x) = x^4 + x + 1$	99
4.4	Two Stage Scrambler; $c(x) = x^2 + x + 1$	112
4.5	Three Stage Scrambler; $c(x) = x^3 + x + 1$	125
4.6	Four Stage Scrambler; $c(x) = x^4 + x + 1$	141
4.7	Five Stage Scrambler; $c(x) = x^5 + x^2 + 1$	149

ABSTRACT

In data communication systems periodic data streams occur due to (a) transmission of periodic sequences during idle condition for ensuring efficient timing recovery, (b) transmission of training sequences where adaptive equalization is incorporated at the receiver and (c) periodicity in the message itself. The presence of periodic sequences may lead to certain difficulties which are dependant either on the period of the data or on pattern thereof. These are, (a) single tone interference in adjacent channel produced because of the periodic data streams, (b) inefficient adaptive equalization resulting due to short periodic data streams and (c) inefficient timing recovery resulting either due to infrequent changes in amplitude of the data or due to absence of densely spaced line spectrum during the idle period, depending upon the type of timing recovery scheme adapted. A device called "scrambler" is used to circumvent them.

In this thesis we study the performance of binary digital data scramblers for periodic input sequences with respect to the period of the output sequence and spectral coefficients of input and output sequences. The periodic analysis of the output of the scrambler is based on D-transform techniques using the properties of polynomials and partial fraction expansion of partial fraction expansion of rational functions of polynomials over  $GF(2)$ . The spectral analysis of input and output sequences is based on spectral theory of linear sequential circuits over finite fields. It is shown that (a) if the period  $s$  of the input sequence is not a multiple of the period  $q$  of zero input response of the

scrambler, the output period is of period equal to the least common multiple of  $s$  and  $q$  except for a unique state for which the output period is  $s$  itself and (b) if the period  $s$  is a multiple of  $q$  then the period of the output sequence is also a multiple of  $q$ . It is observed that for a  $n$ -stage scrambler (a) eigenvalues for all eigensequences over an extension field  $GF(2^m)$  is defined if  $n$  is not a divisor of  $m$ ; otherwise eigenvalues are not defined for  $n$  eigensequences, (b) spectral coefficients corresponding to eigensequences for which eigenvalues are not defined, are zero for those input sequences of period  $s$  ( $s$  equal to or a divisor of  $2^n-1$ ); the new spectral coefficients, if any, appearing in the output sequence at these locations are due to the zero input response for a state determined by, the unique states corresponding to eigensequences having non-zero coefficients at the input and initial state of the scrambler, and (c) for other input and output sequences both having periodicities equal to or a divisor of  $2^i-1$ ,  $i$  is not equal to  $n$ , no new spectral coefficients appear at output other than those determined by input coefficients and respective eigenvalues.

## CHAPTER 1

### INTRODUCTION

In data communication systems periodic data streams may occur due to

- (a) transmission of periodic sequences during idle condition for ensuring efficient timing recovery,
- (b) transmission of training sequences where adaptive equalization is incorporated at the receiver, and
- (c) periodicity in the message itself.

The presence of periodic sequences may lead to certain difficulties which are dependant either on the period of the data or on pattern thereof. These are,

- (a) Single tone interference in adjacent channel produced because of the periodic data streams.
- (b) Inefficient adaptive equalization resulting due to short periodic data streams.
- (c) Inefficient timing recovery resulting either due to infrequent changes in amplitude of the data or due to absence of densely spaced line spectrum during the idle period, depending upon the type of timing recovery scheme adapted.

In this chapter we illustrate these difficulties and describe a device called "Scrambler" which is used to circumvent them.

### 1.1 Spectrum of Periodic Data

Consider a gating function as shown in Figure 1.1. For the ease of illustration let us assume that the period is some multiple of the pulse width  $\delta$ . Expanding this function using exponential Fourier series, its spectral components are given by

$$F_n = \frac{A}{T} \text{Sa} \left( \frac{n\pi\delta}{T} \right) \quad (1.1)$$

where  $n = \dots, -2, -1, 0, 1, 2, \dots$  and  $\text{Sa}(x)$  is sampling function. The frequency spectrum is shown in Figure 1.2. The fundamental frequency is  $2\pi/T$ . The frequency spectrum is a discrete function and exists only at  $\omega = 0, \pm \frac{2\pi}{T}, \pm \frac{4\pi}{T}, \dots$  and has amplitudes  $\frac{A}{T}, \frac{A}{T} \text{Sa}(\frac{\pi\delta}{T}), \frac{A}{T} \text{Sa}(\frac{2\pi\delta}{T}), \dots$  respectively.

Now consider a periodic data  $\dots, 1001, 1001, \dots$  as shown in Figure 1.3. This can be considered as made up of a gating function  $f(t)$  and a shifted gating function  $f(t - 3\delta)$ . The spectral components of  $f(t - 3\delta)$  are given by

$$\begin{aligned} F'_n &= \frac{A\delta}{T} \text{Sa} \left( \frac{n\pi\delta}{T} \right) e^{-j\omega(3\delta)} \\ &= \frac{A\delta}{T} \text{Sa} \left( \frac{n\pi\delta}{T} \right) e^{-j\frac{6n\pi\delta}{T}} \end{aligned} \quad (1.2)$$

The discrete frequency components which appear in  $f(t - 3\delta)$  are same as those in  $f(t)$ . If we denote the spectral components of the sequence  $\dots, 1001, 1001, \dots$  by  $F''_n$  then

$$F''_n = F_n + F'_n \quad (1.3)$$

Amplitudes of any discrete frequency may get added up or get reduced since the phase angle is involved. There is **atleast**

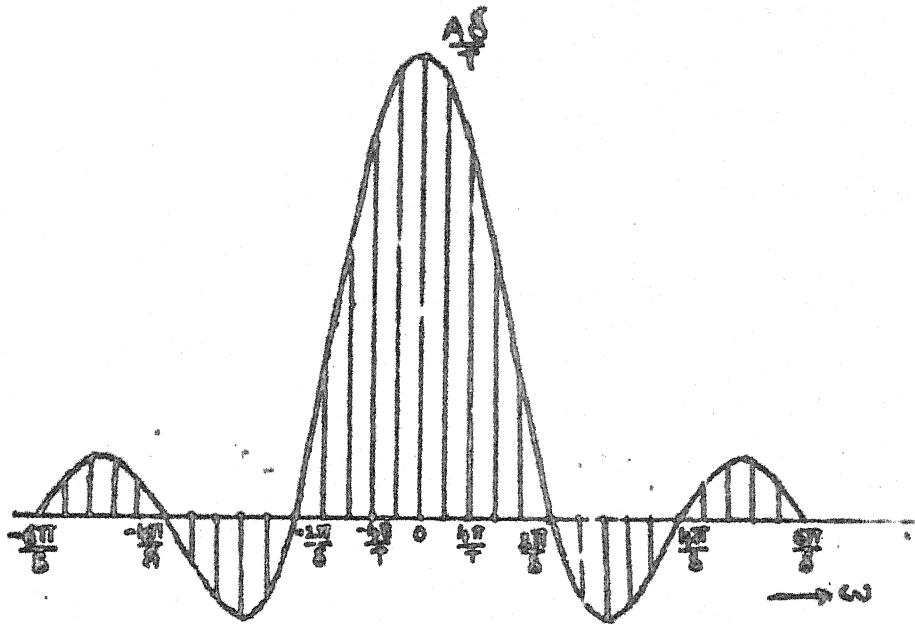


Fig 1.2 Spectrum of Gating Function

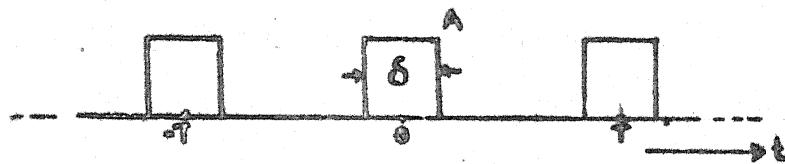


Fig 1.1 Gating Function

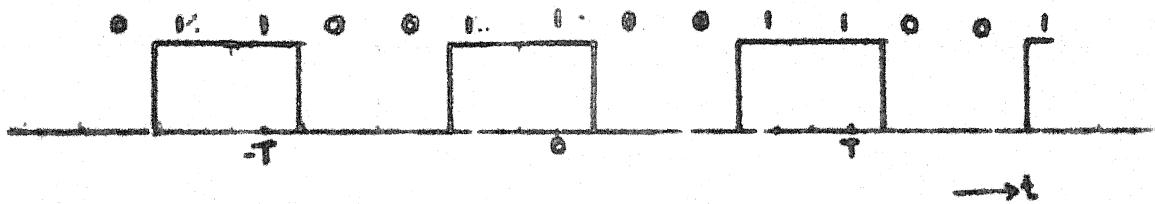


Fig 1.2 Data Stream ...1001...

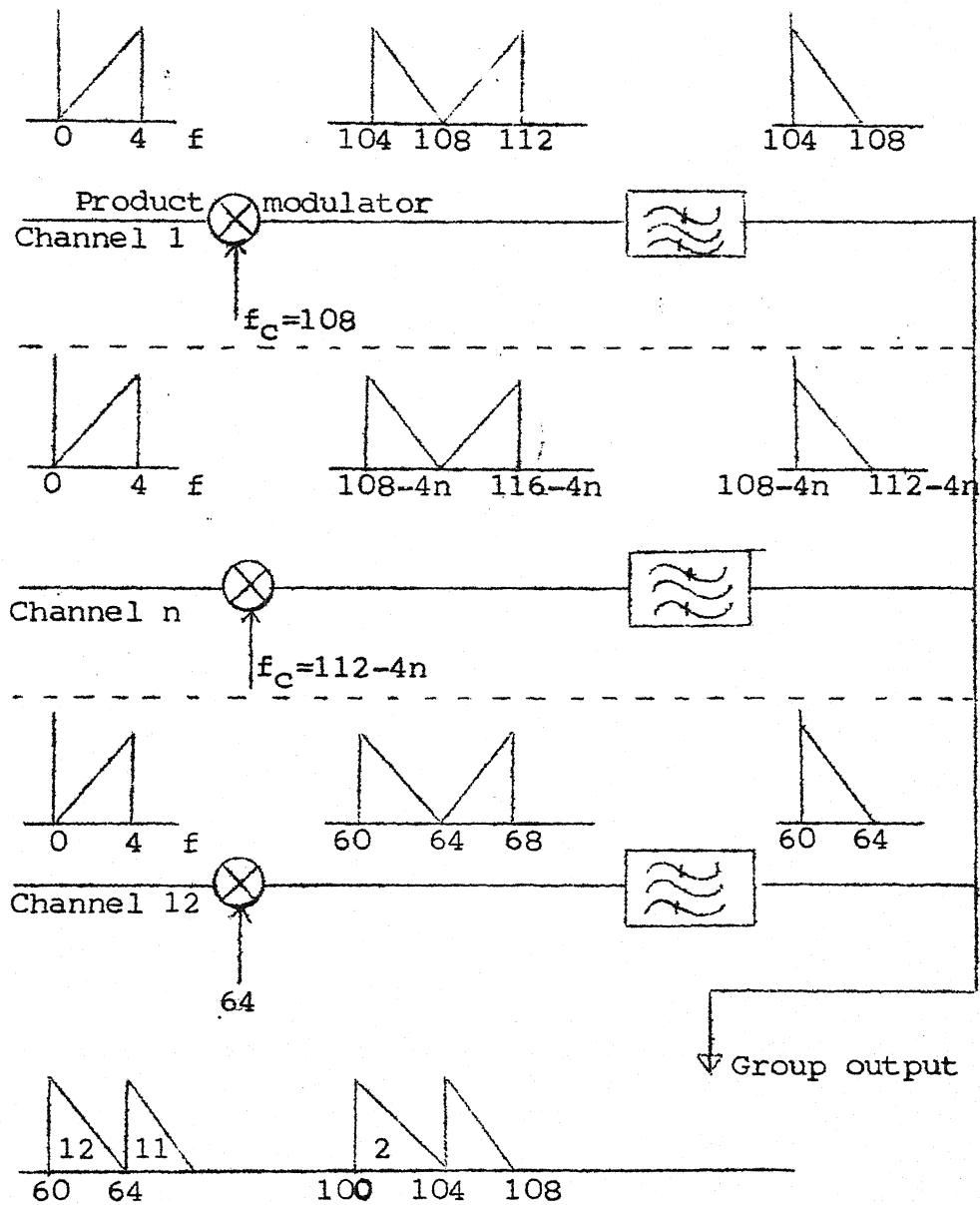
one frequency component i.e. DC component the amplitude of which always gets added up (ofcourse this is not the case in bipolar signalling). In any case, amplitudes are inversely proportional to period  $T$ . Also note that as  $T$  increases, the spectrum becomes densely spaced.

### 1.2 Single Tone Interference

Now consider a typical basic group modulation scheme in a carrier communication system shown in Figure 1.4 [16]. Let us assume that channel 1 has a device which introduces square law nonlinearity before modulation taking place. A tone of 2.5 KHz (say) in this channel gives rise to its second harmonic i.e. a 5 KHz tone. This 5 KHz tone after modulation appears at 103 KHz, i.e. in the domain of channel 2 (100 KHz - 104 KHz) and causes interference. This is called as 'Single Tone Interference'. For this reason, system engineers place limits on the levels of isolated tones in a customer's transmission band. From previous section it is clear that tones are produced in data transmission system by periodic data sequences. Because of the inverse relation, the upper bound on tone levels is then gets translated to a lower bound on the period of the data sequence. Hence it is desirable to map any source sequence on to a periodic channel sequence of larger period.

### 1.3 Adaptive Equalization

Consider the block diagram of a communication system shown in Figure 1.5. For distortionless transmission of signal, it must experience a specified constant amount of gain or loss



Note: All frequencies in KHz.

Figure 1.4 Basic Group Modulation Scheme.

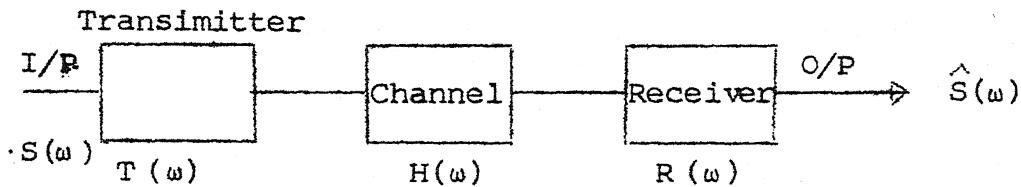


Figure 1.5 Block Diagram of a Communication System.

and a linear phase shift i.e.

$$\hat{S}(\omega) = K S(\omega) e^{j\omega t_0} \quad (1.4)$$

where  $K$  and  $t_0$  are constants. This will be satisfied only if

$$X_{eq}(\omega) = T(\omega) H(\omega) R(\omega) = K e^{j\omega t_0} \quad (1.5)$$

But in real systems, this is not the case as  $X_{eq}(\omega)$  is given by

$$X_{eq}(\omega) = K(\omega) e^{j\phi(\omega)} \quad (1.6)$$

This deviation from the ideal transmission characteristic causes distortion of input signal which causes overlapping between successive symbols in data communication and is known as 'Intersymbol Interference' (ISI). This can be combated by using a device called equalizer as indicated in Figure 1.6.

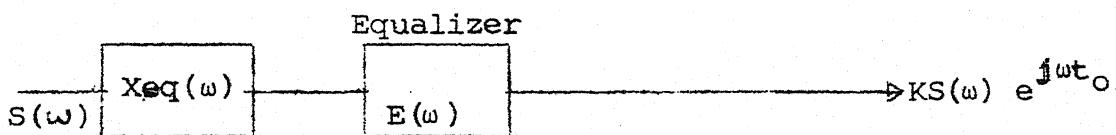


Figure 1.6 Block Diagram of a Communication System with Equalizer.

The transfer function  $E(\omega)$  of the equalizer should be

$$E(\omega) = \frac{K}{x_{eq}(\omega)} e^{-j\phi(\omega) - \omega(t_o - t'_o)}, \text{ for all } \omega \quad (1.7)$$

$$\text{Then } \hat{S}(\omega) = S(\omega) x_{eq}(\omega) E(\omega) = K S(\omega) e^{j\omega t'_o} \quad (1.8)$$

At high data rates - 4800 bits/sec and above - where the channel characteristics vary slowly compared to data rate, the setting of the equalizer is automatically adjusted to match the channel. This is known as 'adaptive equalization'. In the next section, we will see how the equalization gets degraded because of the presence of short periodic sequences in the data.

#### 1.4 Spectrum of the Received Signal [5]

Now consider a digital transmission scheme illustrated in the Figure 1.7. Assuming an ideal channel, the signal

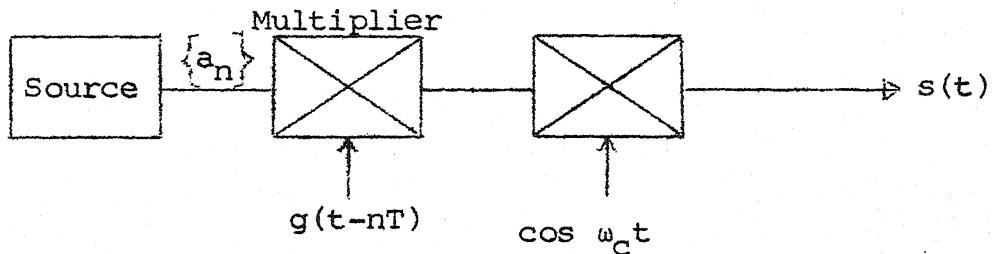


Figure 1.7 Block Diagram of a Digital Transmission Scheme.

$s(t)$  received at the receiver is given by

$$s(t) = \sum_n a_n g(t - nT) \cos \omega_c t \quad (1.9)$$

Let  $\{a_n\}$  be periodic with the period  $N$ . The DFT of  $\{a_n\}$  is given by

$$A(k \Omega) = \sum_{n=0}^{N-1} a_n e^{-jkn \Omega T} \quad k = 0, 1, \dots, N-1 \quad (1.10)$$

and the inverse relation is

$$a_n = \frac{1}{N} \sum_{k=0}^{N-1} A(k \Omega) e^{jkn \Omega T}, \quad n = 0, 1, \dots, N-1 \quad (1.11)$$

where  $T$  is the symbol duration and  $\Omega = \left(\frac{1}{N}\right)\left(\frac{2\pi}{T}\right) = \frac{1}{N} \omega_s$

where  $\omega_s$  is symbol frequency in rad/sec. Hence the DFT has  $N$  components uniformly spaced  $\frac{1}{NT}$  Hz apart and the spectrum repeats every  $\frac{1}{T}$  Hz. The spectrum  $S(\omega)$  of  $s(t)$  is given by

$$S(\omega) = \pi \left[ \sum_n a_n e^{-j\omega nT} G(\omega) \right] * \delta(\omega - \omega_c), \quad \omega > 0 \quad (1.12)$$

and using Equation (1.11) in Equation (1.12) we obtain,

$$\begin{aligned} S(\omega) &= \pi \left[ \sum_n \frac{1}{N} \sum_{k=0}^{N-1} A(k \Omega) e^{jkn \Omega T} e^{-j\omega nT} G(\omega) \right] * \delta(\omega - \omega_c) \\ &= \frac{1}{N} \sum_{k=0}^{N-1} A(k \Omega) \left[ \sum_n e^{-j(\omega - k\Omega)nT} G(\omega) \right] * \delta(\omega - \omega_c) \end{aligned} \quad (1.13)$$

Using the identity  $\sum_n e^{-j\omega nT} = \left(\frac{2\pi}{T}\right) \sum_n \delta(\omega - \frac{2\pi n}{T})$  in Equation (1.13) gives,

$$S(\omega) = \frac{2\pi^2}{NT} \sum_{k=0}^{N-1} A(k \Omega) \left[ \sum_n \delta(\omega - k\Omega - n\omega_s) G(\omega) \right] * \delta(\omega - \omega_c)$$

i.e.

$$S(\omega) = \frac{2\pi^2}{NT} \sum_{k=0}^{N-1} A(k \Omega) \left[ \sum_n G(k \Omega + n\omega_s) \delta(\omega - \omega_c - k\Omega - n\omega_s) \right] \quad \omega > 0$$

or

$$S(\omega) = \frac{2\pi^2}{NT} \sum_{k=0}^{N-1} A(k \Omega) \left[ \sum_n G(k \Omega + n\omega_s) \delta(\omega - \omega_c - k\Omega - n\omega_s) \right] \quad (1.14)$$

It is clear that  $S(\omega)$  has discrete tones at  $\omega_c + k\Omega + n\omega_s$ . In particular data transmission systems with pulses of less than 100% excess band width,  $G(k\Omega + n\omega_s)$  will be zero if  $n$  is not equal to zero or -1. Hence for  $n = 0$  and -1,

$$S(\omega) = \frac{2\pi^2}{NT} \sum_{k=0}^{N-1} A(k\Omega) \left[ G(k\Omega) \delta(\omega - \omega_c - k\Omega) + G(k\Omega - \omega_s) \delta(\omega - \omega_c - k\Omega + \omega_s) \right], \quad \omega > 0 \quad (1.15)$$

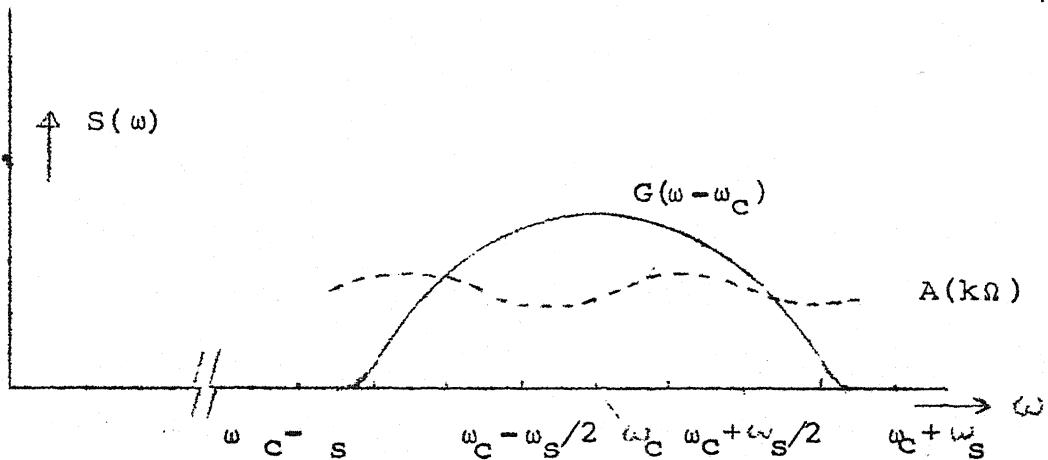


Figure 1.8 Spectrum given in Equation (1.15).

The spectrum is illustrated in Figure 1.8. It is clear that the envelope  $A(k\Omega)$  modulates the base band pulse shape  $G(\omega - \omega_c)$ , in the range  $\omega_c - \omega_s$  to  $\omega_c + \omega_s$ .

In adaptive equalization, since  $s(t)$  is used to adjust the tap weights, it is obvious that a constant  $A(k\Omega)$  envelope will be ideal.  $A(k\Omega)$  has frequency components at discrete points and hence the equalization can be achieved only at those discrete frequencies which are in the range of  $-\omega_s$  to  $\omega_s$ . For example if the period were two symbol intervals (i.e.  $2T$ ), from Figure 1.2 it is clear that there are only two discrete frequency components one at  $-\frac{\omega_s}{2}$  and the other at  $+\frac{\omega_s}{2}$  in the Nyquist

band. Hence the equalizer can correct for distortion only at these two points. Consequently at the instant when the data returns from the periodic to the random mode, the equalizer tap settings will be far from their optimum (for random data) values, and the distortion at the equalizer output could be larger than the channel distortion. Hence it is desirable that if there are any periodic sequences in the data, it is to be mapped to a sequence of larger periodicity so that its spectrum is denser and hence equalizer is kept 'trained'.

### 1.5 Timing Recovery from Zero Crossings [14]

Timing recovery is one of the most critical function performed by a synchronous modem in data communication system. There are various schemes. But most modems derive their timing frequency from amplitude transitions in the received signal. One such scheme is shown in Figure 1.9.

The clock recovery network consists of a voltage controlled oscillator (VCO) and a phase comparator consisting of the phase comparison logic and transistor controlled current switches. When the input  $s(t) = 0$ , the one shot multivibrator outputs a pulse of duration  $0.5 T$ , where  $T$  is one element duration. This triggers phase comparison logic circuit. The correction or error signal comes out of the phase comparator in the form of current  $I_C$ . This controls the charging and discharging of the capacitor and the voltage across the capacitor controls the VCO, generating the clock signal.

From the timing diagram it is clear that at time  $t_1$ , the clock signal is in phase and between time  $t_1$  and  $t_2$  the

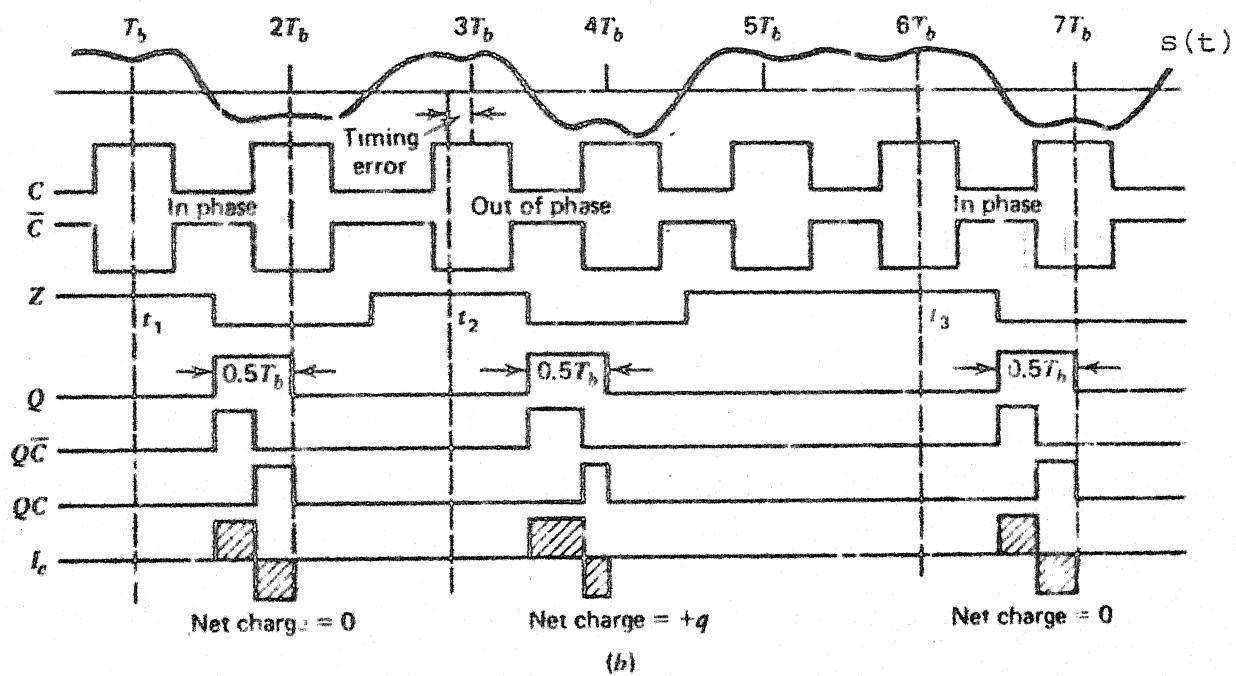
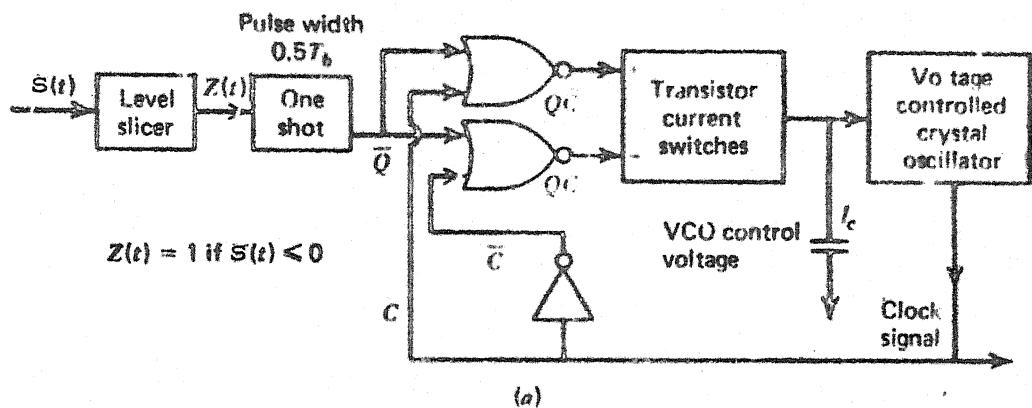


Figure 1.9 Timing Recovery Scheme.

clock signal drifts by a small amount. As  $s(t)$  goes negative at  $t_1$ , the one shot is triggered and it produces a pulse of duration  $0.5 T$ . The phase comparison logic generates two equal width pulses  $Q_C$  and  $Q\bar{C}$ , and the current  $I_C$  has a waveform with equal width, equal amplitude positive and negative portions. The net change in the charge across the capacitor is zero, the VCO control voltage remains constant, and no adjustment is made on the rate and phase of the clock signal.

As the clock signal drifts out of phase, the phase comparison operation at time  $t_2$  results in a current pulse  $I_C$  with a more positive component. Now there is a change in the capacitor charge and hence a change in the VCO control voltage. This change in the VCO control voltage results in a correction of the clock phase. In the figure, the clock phase is shown - corrected at  $t_3$ , before the next phase comparison operation is initiated.

One point to be noted here is that the phase comparison and correction operation is initiated by zero crossings in the received waveform  $s(t)$ . Hence the performance of this timing wave regenerator will degrade considerably if the signal stays at a constant level for long periods of time. In other words, such an arrangement cannot handle all possible sequences of data. We say such a system is not "transparent" for certain data sequences. Thus it is desirable to map a source sequence on to a line sequence which has many closely spaced transitions. Also during idle period there should be some line sequence transmitted which has closely spaced transition.

1.6 Precession and Its Effect on the Timing Recovery 5

Consider a phase modulated signal  $s(t)$ , given by

$$s(t) = \sum_{n=-\infty}^{\infty} g(t - nT) \cos(\omega_c t + \theta_n) \quad (1.16)$$

whose idle code is  $\theta_n = 0$  for all  $n$ . In the previous section we have obtained

$$s(\omega) = \frac{2\pi^2}{NT} \sum_{k=0}^{N-1} A(k\Omega) \left[ \sum_n G(k\Omega + n\omega_s) \delta(\omega - \omega_c - k\Omega - n\omega_s) \right] \quad \omega > 0 \quad (1.14)$$

For convenience, we will write Equation (1.16) as

$$s(t) = \sum_{n=-\infty}^{\infty} \{a_n\} g(t - nT) \cos \omega_c t \quad (1.17)$$

during idle period; where  $a_n$  is a sequence of all 1 throughout.

This can be incorporated in Equation (1.14) by letting  $A(k\Omega) = k_0$  and  $N = 1$ . Hence

$$s(\omega) = \frac{2\pi^2}{T} \sum_n G(n\omega_s) \delta(\omega - \omega_c - n\omega_s) \quad (1.18)$$

For an excess band width of less than 100%,  $G(n\omega_s)$  will be zero for  $n \neq 0$ . Hence

$$s(\omega) = \frac{2\pi^2}{T} G(0) \delta(\omega - \omega_c) \quad (1.19)$$

It is clear that  $s(\omega)$  contains a single tone and hence it is not possible to obtain a timing tone during idle condition, refer Figure 1.10(a).

Now let us consider how this situation can be avoided by employing differential phase modulation with precession. In

a differential phase modulation, the phase of the carrier during the transmission of the  $n^{\text{th}}$  message symbol is given by

$$\theta_n = \theta_{n-1} + \phi_n$$

where  $\phi_n$  is any one of the  $\frac{M}{2}$  equally spaced angles;  $\frac{M}{2}$  is the alphabet size. The advancing of the phase of the carrier by  $\frac{2}{M}$  radians independently of any change in the input data is known as precession. With precession  $\theta_n$  can be written as

$$\theta_n = \theta_{n-1} + \phi_n + \frac{2n\pi}{M} \quad (1.20)$$

During idle period  $\phi_n = 0$ . Assuming  $\theta_{n-1} = 0$ , we can write

$$\theta_n = \frac{2n\pi}{M}, \quad (1.21)$$

and has period  $M$ . Hence during idle period we can write

$$s(t) = \operatorname{Re} \left\{ e^{j\theta_n} g(t - nT) e^{j\omega_c t} \right\} \quad (1.22)$$

$$\text{i.e. } a_n = e^{j\theta_n} = e^{j(2n\pi/M)} \quad (1.23)$$

$$\begin{aligned} \therefore A(k\Omega) &= \sum_{n=0}^{M-1} a_n e^{-jnk(2\pi/M)} \\ &= \sum_{n=0}^{M-1} e^{-j(2\pi/M)n(k-1)} = \delta_{k-1} \end{aligned} \quad (1.24)$$

Substituting this in Equation (1.14), we get

$$S(\omega) = \sum_n G(n\omega_s + \frac{\omega_s}{M}) \delta(\omega - \omega_c - \frac{\omega_s}{M} - n\omega_s) \quad (1.25)$$

Thus the effect of precession is to offset the tones by  $\frac{\omega_s}{M}$ , producing the spectrum shown in Figure 1.10(b). Hence when  $s(t)$  is squared, it provides a tone at 1200 Hz.

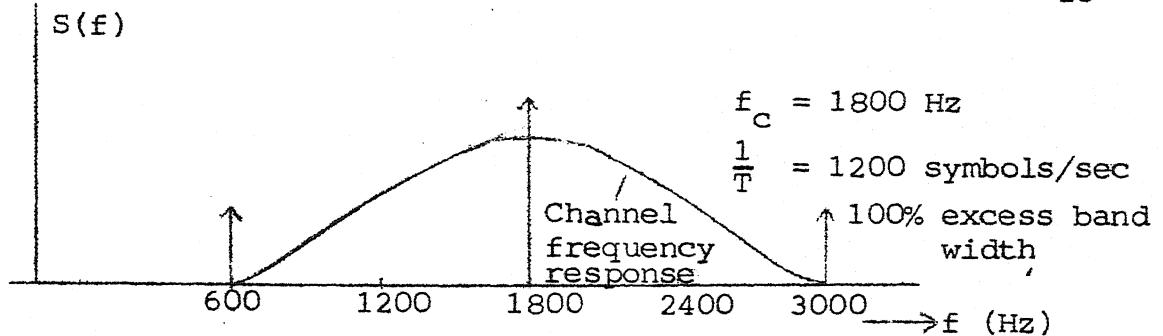


Figure 1.10(a) Spectrum Without Precession.

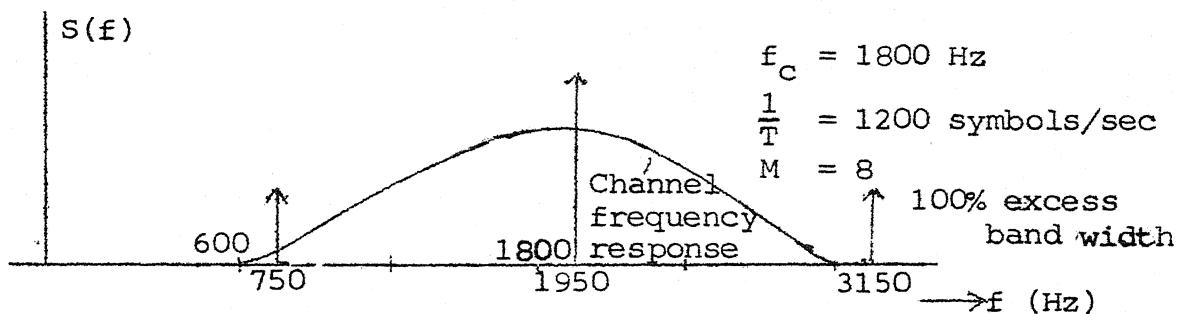


Figure 1.10(b) Spectrum With Precession.

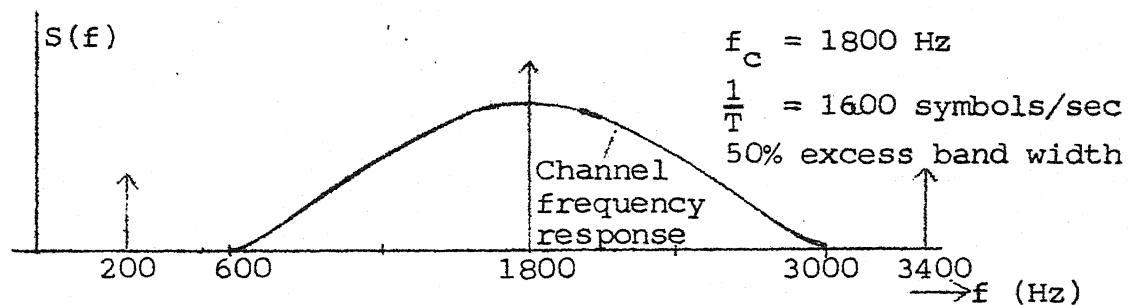


Figure 1.11(a) Spectrum Without Precession.

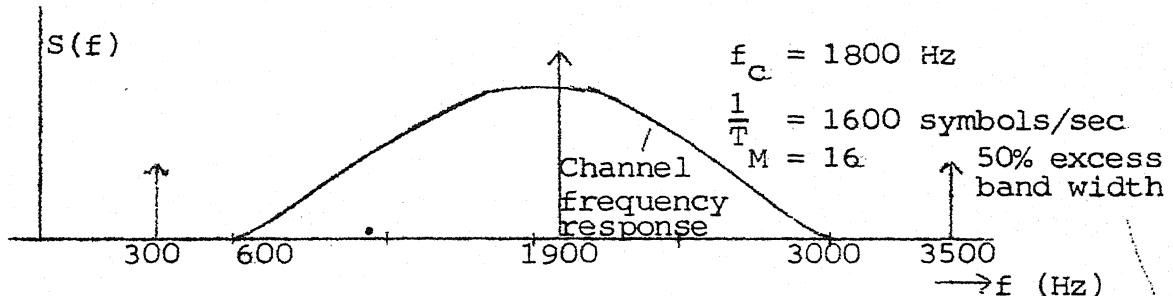


Figure 1.11(b) Spectrum With Precession.

Now consider a situation of only 50% excess band width as shown in Figure 1.11(a), with  $\theta_n = 0$ . The spectrum with precession shifts the tones by  $\frac{\omega_s}{M}$  i.e. by 100 Hz in this case as shown in Figure 1.11(b). Still there is only one inband tone. Hence for the systems with a very small excess band width it is not possible to recover timing frequency even with precession. Therefore for high speed data transmission, where the excess band width is quite small, employing differential phase modulation, spectral enrichment of  $A(k\Omega)$  is necessary to ensure timing recovery.

Now let us see in the context of binary data communication what is implied by saying spectral enrichment of sequence  $\{a_n\}$ . The block diagram of a differentially phase shift keying modulator is shown in Figure 1.12 [12]. The differential encoding operation performed by the modulator is explained in Table 1.1. The encoding operation starts with an arbitrary first bit, say 1 and thereafter the encoded bit stream  $\{d_n\}$  is generated by

$$d_n = d_{n-1} b_n + \bar{d}_{n-1} \bar{b}_n \quad (1.26)$$

and the sequence  $\{a_n\}$  is given by

$$\{a_n\} = \begin{cases} 1 & \text{if } d_n = 1 \\ -1 & \text{if } d_n = 0 \end{cases} \quad (1.27)$$

The encoding operation during idle condition (space idle condition is assumed) is explained in Table 1.2. It is clear that the sequence  $\{a_n\}$  is periodic with period as two element

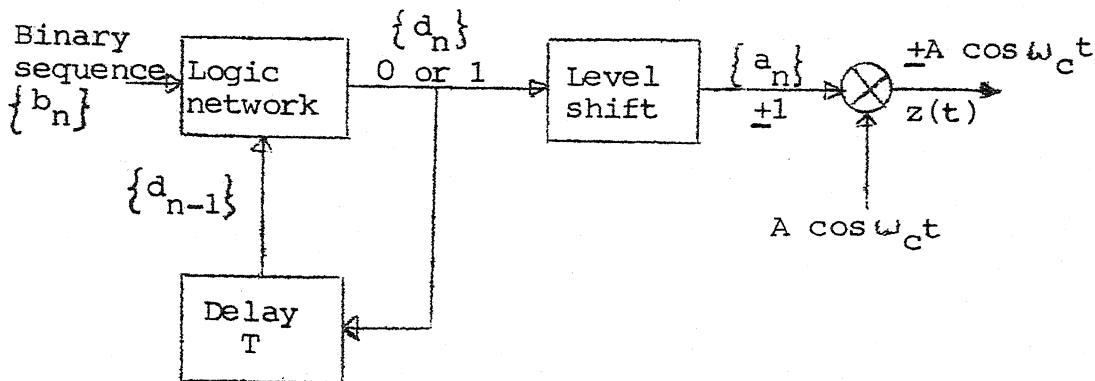


Figure 1.12 DPSK Modulator.

Table 1.1 Differential Encoding

Input sequence $\{b_n\}$	1	1	1	0	1	0	0	0	1	1
Encoded sequence $\{d_n\}$	1*	1	1	0	0	1	0	1	1	1
Encoded sequence $\{a_n\}$		1	1	-1	-1	1	-1	1	1	1
Transmitted phase	0	0	0			0		0	0	0

\* Arbitrary starting reference bit.

Table 1.2 Differential Encoding - Space Idle Condition

Input sequence $\{b_n\}$	0	0	0	0	0	0	0	0
Encoded sequence $\{d_n\}$	1*	0	1	0	1	0	1	0
Encoded sequence $\{a_n\}$		-1	1	-1	1	-1	1	-1
Transmitted phase	0	0		0		0		0

\* Arbitrary starting reference bit.

duration. From Section 1.1 it follows that the spectrum of  $\{a_n\}$  will be enriched if it is mapped to a sequence of larger period.

### 1.7 Scrambler

From Sections 1.2 and 1.4 to 1.6 it is clear that the data sequence should not consist of short periodic sequences as well as longer durations of constant amplitude. This is achieved by interposing a device called "Scrambler" between the data source and the modulator. Its purpose is to map any periodic source sequence to a line sequence of larger period and to ensure a line sequence with closely spaced transitions during the time when source sequence consists of longer durations of constant amplitude. A descrambler is inserted between the demodulator and the data sink, to undo what scrambler at the transmitter end did, to get back the original source sequence.

The system block diagram is shown in Figure 1.13, where  $\{b_n\}$  is

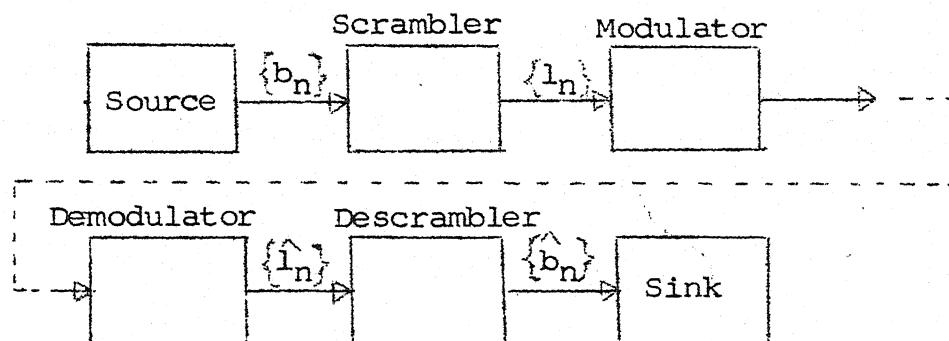


Figure 1.13 Block Diagram of a Communication System with Scrambler.

the source sequence and  $\{l_n\}$  is the line sequence. If there are no errors, the detected line sequence  $\{\hat{l}_n\}$  will be same as  $\{l_n\}$  and in that case  $\{\hat{b}_n\}$  will be nothing but  $\{b_n\}$ , the transmitted source sequence.

A method of scrambling binary data is shown in Figure 1.14. A binary maximal length sequence (M-sequence) is generated using a feed back shift register and is added (modulo 2) bit by bit to the data string. The data is descrambled by repeating the procedure using an identical synchronised shift register. The source sequence is recovered at the descrambler if the state of the random sequence generators at both ends is synchronised. There is no way of automatic synchronisation and hence this is required to be achieved by external means, may be by providing additional channel or circuitry.

### 1.8 Self Synchronising Scramblers

Savage [14] proposed two types of scrambler equipped with M-sequence generators and having self synchronising property. Hence they are termed as self synchronising scramblers. The two types differ only in their "monitoring logic" used to detect and eliminate any sequence of undesirable period at the output of the scrambler. The scrambler and descrambler structure which is basic to both the types are shown in Figures 1.15(a) and 1.15(b) respectively.

In the structures shown in Figures 1.15(a) and 1.15(b), the data is a sequence of digits from the modular field of  $p$  elements,  $0, 1, \dots, p-1$ , where  $p$  is prime. Addition and multiplication is taken modulo  $p$ . The output of the

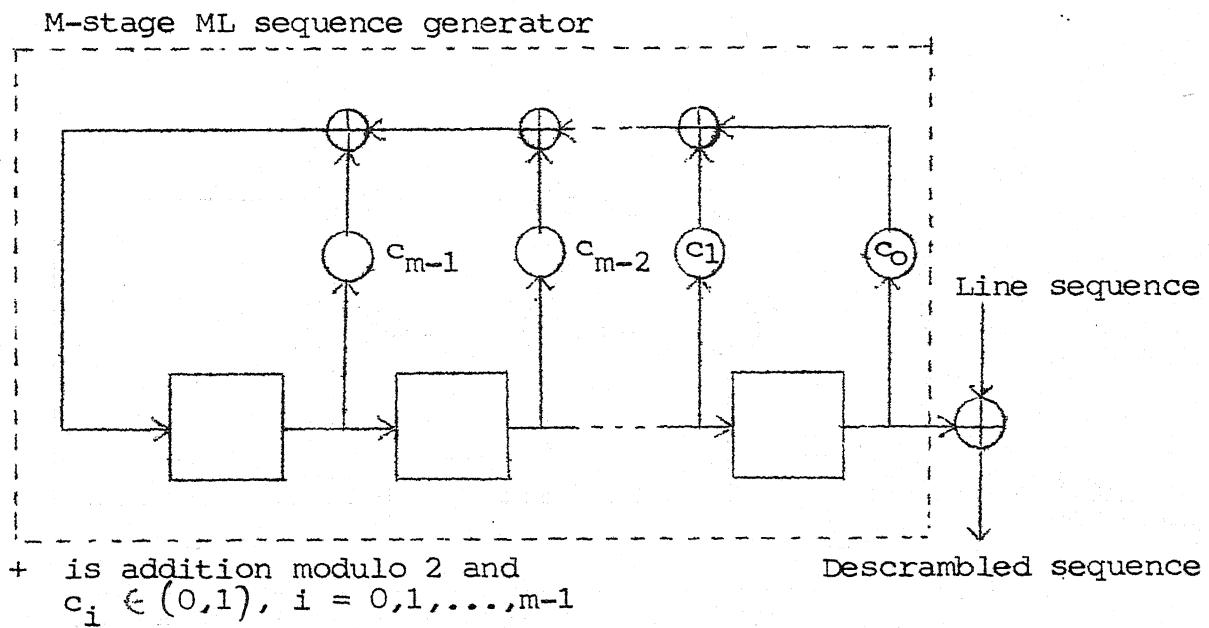
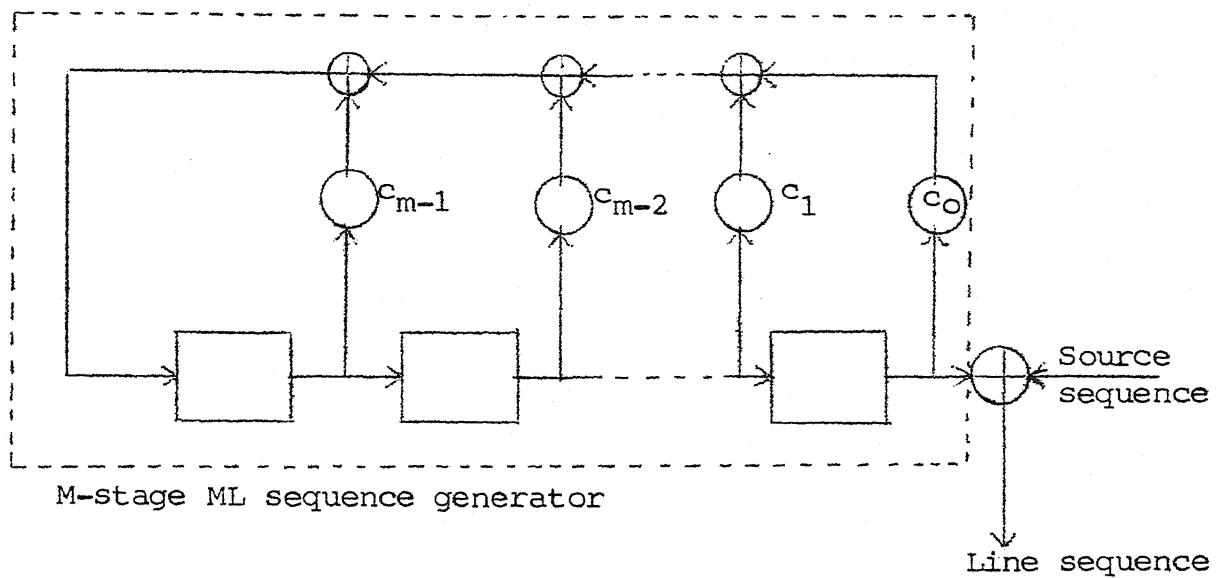


Figure 1.14 A Method of Scrambling Binary Data.

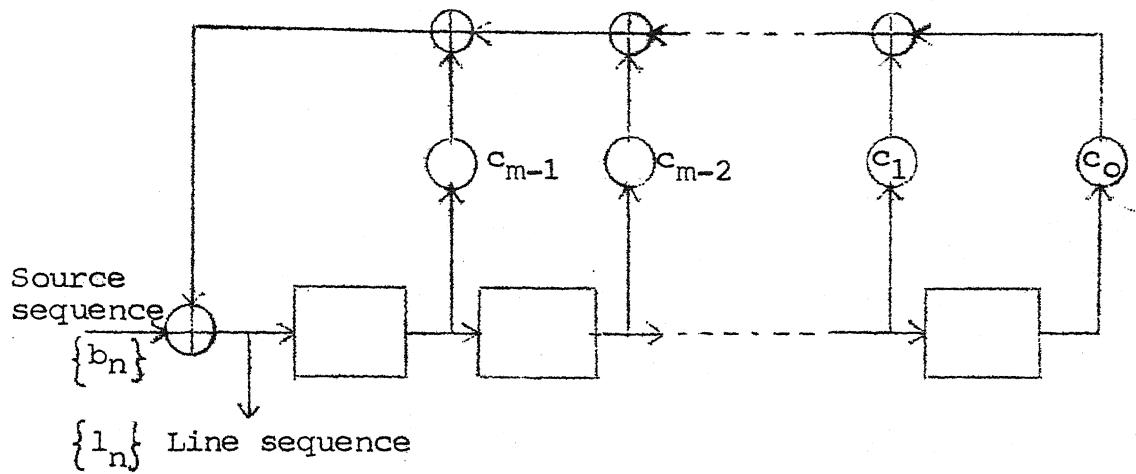


Figure 1.15(a) Basic Scrambler.

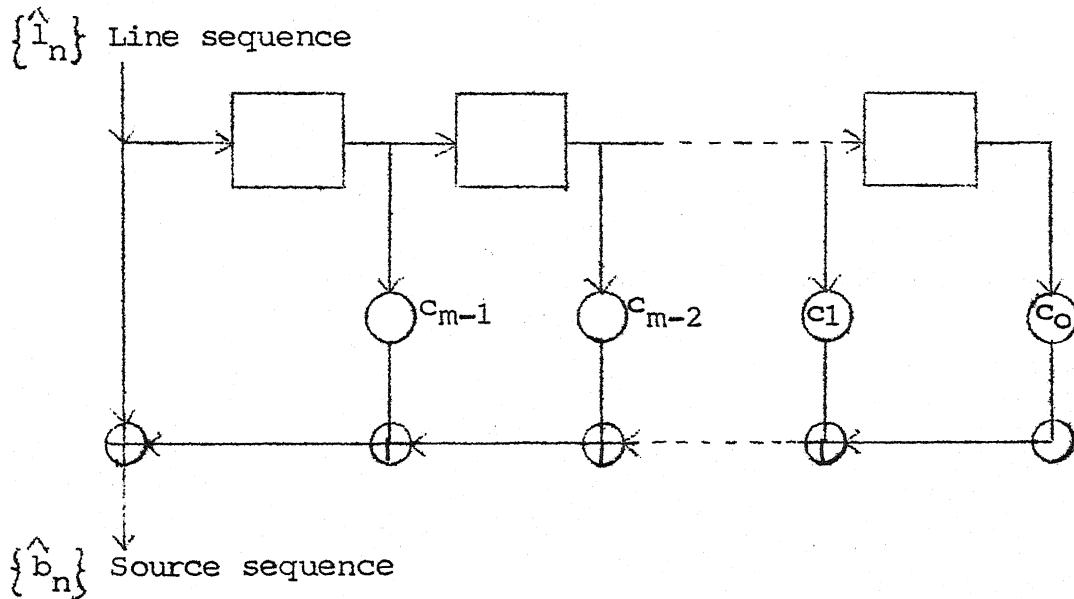


Figure 1.15(b) Basic Descrambler.

storage elements are multiplied by the tap constants ( $c_0, c_1, \dots, c_{m-1}$ ) drawn from  $GF(p)$ . The tap polynomial - also called as characteristic polynomial -  $c(x)$  is given by

$$c(x) = x^m - c_{m-1}x^{m-1} - \dots - c_0 \quad (1.28)$$

is a primitive polynomial over the field  $GF(p)$ . When there is no input, the output sequence of the basic scrambler is all zero if the initial state of the storage elements is all zero and for the non-zero initial state, the output sequence will be a  $M$ -sequence of period  $q = p^m - 1$ . This period we will call as "cycle length". From the Figures 1.15(a) and 1.15(b) we can write

$$l_n = b_n + (c_{m-1}l_{n-1} + c_{m-2}l_{n-2} + \dots + c_0 l_{n-m}) \quad (1.29)$$

and

$$\hat{b}_n = \hat{l}_n - (c_{m-1}\hat{l}_{n-1} + c_{m-2}\hat{l}_{n-2} + \dots + c_0 \hat{l}_{n-m}) \quad (1.30)$$

Assuming error free transmission,  $\{\hat{l}_n\} = \{l_n\}$  and hence

$$\begin{aligned} \hat{b}_n &= l_n - (c_{m-1}l_{n-1} + \dots + c_0 l_{n-m}) + \\ &\quad (c_{m-1} l_{n-1} + \dots + c_0 l_{n-m}) \\ &= b_n \end{aligned} \quad (1.31)$$

From the Figures 1.15(a) and 1.15(b) it is clear that the scrambler-descrambler combination have the self synchronisation property. Any error introduced in the line sequence is felt as long as the values stored in the descrambler disagree with those stored at the scrambler; i.e. for  $m$  bit duration. Also a single error affects as many number of bits as the number

of non-zero tap coefficients in the characteristic polynomial. Hence in practice a primitive polynomial with least number of feed back coefficients is selected as the characteristic polynomial.

Savage has analysed scrambler performance for periodic inputs. He has shown that "the basic scrambler when excited by a periodic sequence of period  $s$  will respond with a periodic line sequence which has either period  $s$  or a period which is the least common multiple (LCM) of  $s$  and  $q$  (LCM ( $s, q$ )) where  $q$  is the cycle length. The period with which the scrambler responds is a function of the initial values stored in the scrambler storage elements, that is, its initial state, and there is but one such state (for each phase of the input sequence) for which the line sequence has period  $s$ . For all other initial states the line sequence has the larger period". We will call that initial state which maintains the period of a sequence as "the critical state" for that sequence.

For the binary case Savage has found lower and upper bounds for the number of transitions in the line sequence when the scrambler is not in the critical state. Also representative calculations are made to determine the spectrum of the scrambler output and it is shown that when the source is periodic, the output spectrum has  $n$  times as many tones as the unscrambled spectrum and each tone has  $1/n^{\text{th}}$  the energy, where  $n$  is the factor by which the source period is increased.

## 1.9 Other Aspects of Scrambler Studies

Apart from these properties of scrambler for periodic input sequences, various other authors have established that in general the statistics of input sequences are improved by scrambler in the sense that the statistics at the output tends towards that of white noise. This is demonstrated by them through autocorrelation and/or power density spectrum.

### 1.9.1 Autocorrelation Function

Nakamura and Iwadare [10] have done analysis of a scrambler equipped with a multilevel M-sequence generator, which is a direct extension of Savage's binary scramblers. Through autocorrelation analysis they established that the scrambler provides considerable randomness to multilevel source sequences.

Henrikson [6] showed that when the input sequence has certain defined randomness, the output digits are uncorrelated everywhere except possibly at symbol separation that are integer multiples of the cycle length. At those points the output autocorrelation is shown to be equal to higher order moments of the input sequence.

### 1.9.2 Power Spectrum

Petrovic [11] obtained a general formula for the power spectrum of a binary signal at the scrambler output. He assumed that the input binary sequence is stationary and statistically independent. His sample calculations of power spectrum confirms the facts established by Henrikson and Kasai et al.

### 1.9.3 Cascaded and Parallel Scramblers

Gitlin et al. [5] studied the input output relationship of scrambler to provide extension to Savage's results. They observed that when the input period is a multiple of the cycle length  $q$ , the output period is  $rq$  independent of the initial state, where  $r = 1, 2, \dots$ . Also they gave a complete description of the output period of a cascaded scrambler as a function of the number of stages. It is shown that the output period does not necessarily double with the addition of a stage and that if a particular scrambler stage does not reach critical state, no succeeding stage will do so. Also, it is proved that the parallel scrambler configuration can, via spectral cancellation, cause the strength of the timing tone to be attenuated.

### 1.9.4 Universal Scrambler

Leeper [8] has shown that it is possible to 'whiten' to any degree all the first- and second-order statistics of any binary source at the cost of an arbitrarily small controllable error rate. He has established that any binary source can be 'whitened' to an arbitrary small first- and second-order probability density imbalance  $\delta$  if (i) the source is first passed through the equivalent of a symmetric memoryless channel with an arbitrarily small but non-zero error probability  $\epsilon$  and (ii) the scrambler contains  $M$  stages where

$$M \geq 1 + \log_2 \left[ (\ln 2\delta) / \ln(1 - 2\epsilon) \right]$$

The structure proposed by him is shown in Figure 1.16.

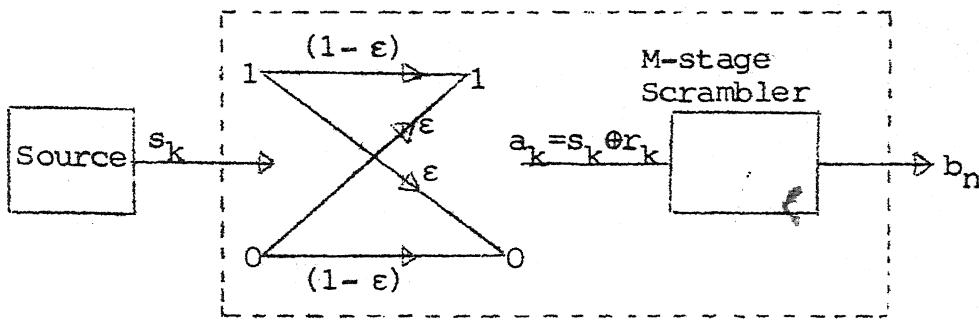


Figure 1.16(a) Universal Scrambler.

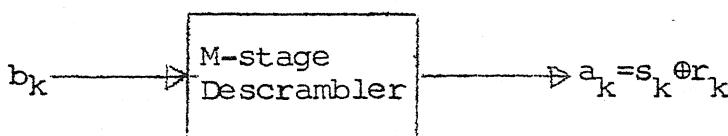


Figure 1.16(b) Descrambler.

Since any binary source can be 'whitened' by this method, he called it as "Universal Data Scrambler".

#### 1.9.5 Systematic Jitter Suppression by Scrambling

Let us again consider the timing recovery scheme shown in Figure 1.5. From the figure it is clear that any obliterations in the zero crossings of the received signal causes change in phase of the clock signal. This clock signal is used to gate the equalized received signal. Hence the obliterations in the zero crossings in effect causes phase modulation of the received signal. This is known as timing jitter. This timing jitter introduced at each repeater gets accumulated in a repeater chain

and may lead to crosstalk and distortion in the reconstructed analog signal. The sources of timing jitter may be classified as systematic or non systematic according to whether or not they are related to pulse pattern. Systematic jitter sources are mainly ISI, finite pulse width, and clock threshold offsets. Kasai et al. [7] showed that the systematic jitter in a PCM repeater chain can be suppressed by incorporating scrambling.

#### 1.9.6 Scrambler for Encryption

Scrambling in general is used to mean encryption for security purposes achieved by adding bit by bit, a M-sequence to a binary data sequence. Analysis of Geffe [3] and Yaralagadda [15] established the fact that any M-sequence generator structure can be obtained by a cryptoanalyst without much difficulty. Hence scrambler in general is not suitable for serious encryption. However by incorporating a nonlinear operation having an inverse operation which can be performed at descrambler, suggested by Arazi [1] makes the task of a cryptoanalyst more difficult.

#### 1.10. Scope of the Work

In this thesis we analyse binary scramblers for periodic input sequences. Various cases considered are, (a) input period not a multiple of cycle length, (b) input period a multiple of cycle length, and (c) input period equal to cycle length. The analysis is based on D-transform techniques, using the properties of polynomials and partial fraction expansion of rational functions of polynomials over  $GF(2)$ .

Also we carry out the spectral analysis of input and output sequences, analogous to Fourier analysis for signals in continuous linear time-invariant system theory, of 2-, 3-, 4- and 5-stage scramblers. This analysis is based on the spectral theory for linear sequential circuits (LSC) suggested by Sangani [13].

#### 1.11. Organisation of the Thesis

In Chapter 1, we discuss certain difficulties which are encountered in data communication systems mainly due to periodic data sequences and data pattern and how this has led to the evolution of self synchronising scramblers. Also we discuss briefly the work carried out by various authors on digital data scramblers.

In Chapter 2, we briefly enumerate certain definitions and properties of Galois fields and of polynomials over these fields. We discuss the notion of formal derivative in Galois fields and its application in obtaining partial fraction expansion of rational functions of polynomials over these fields. At the end of the chapter we state and prove an important Lemma which is made use of in Chapter 3.

In Chapter 3, we analyse the scrambler performance for periodic inputs through D-transform, making use of properties of M-sequence generator and partial fraction expansion of rational functions of polynomials. Through specific illustrations we show how a M-sequence given as input to the scrambler, loses its derivative properties as far as the number of transitions and the cyclic autocorrelation are concerned. We show that under

certain conditions, for a M-sequence generated by the structure other than that of scrambler but of same number of stages, the scrambler acts just as a delay element. Also we show that the partial fraction expansion used throughout in this chapter can have two forms, one complementary to the other. At the end of the chapter we establish that the response of the scrambler for a sequence in critical state can be obtained from the responses due to its constituent sequences when the scrambler is in critical state, and that the critical state for the sequence will be the same linear combination of critical states for constituent sequences. This important result helps us to carry out scrambler analysis in terms of results pertaining only to a set of basis functions.

In Chapter 4, we obtain basis functions for the vector space of periodic sequences of period equal to the cycle length of the scrambler and whose period remains invariant by scrambling. We give a method of obtaining Fourier series expansion for a periodic binary sequence over appropriate extension fields. We briefly discuss the existence of eigensequences and eigenvalues, over an extension field, for LSC defined over finite fields. Based on this we carry out spectral analysis of periodic input and output sequences of 2-, 3-, 4- and 5-stage binary scramblers with eigensequences over extension fields  $GF(2^2)$ ,  $GF(2^3)$ ,  $GF(2^4)$  and  $GF(2^5)$  in each case. Detailed analysis of 5-stage scrambler is given because the two structures in the case of 3- and 4-stage scramblers are reciprocal to each other and are quite likely to give results which probably cannot be generalised.

The last chapter contains conclusions and suggestions for further work on various topics discussed in this thesis.

## CHAPTER 2

### MATHEMATICAL PRELIMINARY

In this chapter, first we briefly enumerate certain definitions and properties of Galois fields and of polynomials over these fields, in Sections 2.1 and 2.2. In Section 2.3 we explain two methods of constructing an extension field  $GF(p^m)$  starting with a ground field  $GF(p)$  and an irreducible polynomial of  $m^{\text{th}}$  degree over  $GF(p)$ . Partial fraction expansion of polynomial fractions over any field is discussed in detail in Section 2.4. An alternative method - similar to the one generally employed for polynomial fractions over the field of real and complex numbers - for polynomial fractions over Galois fields is illustrated in Section 2.5. Material for this chapter are mainly taken from Booth [2] and Gill [4]. At the end we state and prove a Lemma which is used in Chapter 3.

#### 2.1 Galois Field

A field is a set of elements with two operations say, addition and multiplication between any two elements defined such that the set of elements form an abelian group under addition and the set of non-zero elements form a multiplicative abelian group. For example if  $p$  is a prime, the set of integers  $0, 1, \dots, p-1$  with addition and multiplication of any two elements taken modulo  $p$ , form a field. Such a field is represented by  $GF(p)$  and is called "Galois Field" of  $p$  elements.

Example 2.1: The set  $(0,1)$  with addition and multiplication taken modulo 2 constitute  $GF(2)$ . The addition and multiplication tables are given in Table 2.1(a) and Table 2.1(b).

Table 2.1(a) Addition Table for  $GF(2)$

+	0	1
0	0	1
1	1	0

Table 2.1(b)

x	0	1
0	0	0
1	0	1

Example 2.2: The set  $(0,1,2)$  with addition of multiplication taken modulo 3 constitute  $GF(3)$ . The addition and multiplication tables are given in Table 2.2(a) and Table 2.2(b).

Table 2.2(a) Addition Table for  $GF(3)$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 2.2(b)

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Order of an Element: An element  $\beta$  of a field is said to be of order  $k$  if  $k$  is the least non-zero integer such that  $\beta^k = 1$ . The order of any element is a divisor of the number of non-zero elements in the field.

Primitive Element: If in a field, an element generates all the other non-zero elements by repeatedly multiplying by itself then that element is called "primitive element". Its order is

equal to the number of non-zero elements. For example in  $GF(3)$  mentioned above, 2 is a primitive element.

**Characteristic of a Field:** For any element in a field, if  $+ + \dots +$  (p times) = 0, then the field is said to be of characteristic p.

**Extension Field  $GF(p^m)$ :** For every p, a prime and m an integer, there exist a field at  $(p^m)$  with  $p^m$  elements. These are the only finite fields existing.  $GF(p^m)$  is called the extension field of the ground field  $GF(p)$ . Any  $GF(p^m)$  is of characteristic p. Also any  $GF(p^n) \subset GF(p^m)$ , for n, a divisor of m.

**Example 2.3:** The set  $(0, 1, \alpha, \alpha^2)$  with addition and multiplication as defined in Table 2.3(a) and Table 2.3(b) constitute  $GF(2^2)$ .

Table 2.3(a)      Addition Table  
for  $GF(2^2)$

+	0	1	$\alpha$	$\alpha^2$
0	0	1	$\alpha$	$\alpha^2$
1	1	0	$\alpha^2$	$\alpha$
$\alpha$	$\alpha$	$\alpha^2$	0	1
$\alpha^2$	$\alpha^2$	$\alpha$	1	0

Table 2.3(b)      Multiplication  
Table for  $GF(2^2)$

x	0	1	$\alpha$	$\alpha^2$
0	0	0	0	0
1	0	1	$\alpha$	$\alpha^2$
$\alpha$	0	$\alpha$	$\alpha^2$	1
$\alpha^2$	$\alpha^2$	0	$\alpha^2$	1

Note that  $GF(2)$  is contained in  $GF(2^2)$ .

## 2.2 Polynomials Over a Field

A polynomial in x over a field F is an expression of the form  $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$ , where  $f_i \in F$ .

The degree of  $f(x)$  denoted by  $\deg f(x)$  is the greatest  $i$  such that  $f_i \neq 0$ . The degree of polynomial  $f(x) = f_0$  is zero. A polynomial is called 'monic' if the coefficient of the highest power of  $x$  is 1. The set of all polynomials over  $F$  with addition and multiplication of polynomials carried out as in normal polynomial multiplication, with the multiplication and addition operations between the coefficients replaced by field operations, forms a ring. This ring is denoted by  $F[x]$ .

**Division Algorithm:** For any  $a(x)$  and  $b(x)$  in  $F[x]$ , one can write uniquely,

$$a(x) = q(x) b(x) + r(x), \quad 0 \leq \deg r(x) < \deg b(x) \quad (2.1)$$

If the only divisors of  $a(x)$  are  $\alpha$  or  $\alpha a(x) - \alpha$  is an element from  $F$ , then  $a(x)$  is said to be irreducible.

**Greatest Common Divisor (GCD):** The greatest common divisor of two polynomials is the monic polynomial of greatest degree which divides both of them. Let  $a_0(x)$  and  $a_1(x)$  be two polynomials then with some  $b_0(x)$  and  $b_1(x)$  it is possible to write

$$\text{GCD}(a_0(x), a_1(x)) = b_0(x) a_0(x) + b_1(x) a_1(x) \quad (2.2)$$

**Relatively Prime Polynomials:** Two polynomials are said to be relatively prime if their GCD is 1.

**Primitive Polynomial:** Every irreducible polynomial  $f(x)$  indivisible by  $x$  is a factor of  $1-x^i$  for some integer  $i$ . The least such positive integer  $i$  is called the exponent ( $e$ ) of  $f(x)$ . The exponent of a constant is 1. If  $f(x)$  is of degree

$n$  and is irreducible then its exponent is a divisor of  $p^n - 1$ .

Any irreducible polynomial of degree  $n$  and of exponent  $p^n - 1$  is called a primitive polynomial. For every integer  $n$  and prime  $p$ , there is at least one primitive polynomial.

Example 2.4: (i) Consider  $f(x) = x^4 + x^3 + x^2 + x + 1$  over  $GF(2)$ .  $f(x)$  is irreducible and is of exponent 5 ( $\neq 2^4 - 1 = 15$ ). Hence  $f(x)$  is not primitive.

(ii) Consider  $f(x) = x^4 + x + 1$  over  $GF(2)$ . This is irreducible and of exponent 15; i.e.  $f(x)$  divides  $x^{15} + 1$ , and not any  $x^i + 1$  for  $i < 15$ . Therefore  $f(x)$  is primitive.

Unique Factorization Theorem: Every non constant polynomial can be written in the form

$$f(x) = \alpha [f_1(x)]^{k_1} [f_2(x)]^{k_2} \dots [f_r(x)]^{k_r}; \quad k_1 > 0 \quad (2.3)$$

where  $\alpha$  is an element from  $F$  and the  $f_i(x)$  are distinct irreducible, monic, non constant polynomials over  $F$ . Except for ordering,  $f_i(x)$  are unique. The  $[f_i(x)]^{k_i}$  are called the prime factors of  $f(x)$ .

Reciprocal Polynomial: The reciprocal polynomial  $\tilde{f}(x)$  of  $f(x)$  of degree  $n$  is defined as  $x^n f(\frac{1}{x})$ . The exponent of  $\tilde{f}(x)$  is same as that of  $f(x)$ . The prime factors of  $\tilde{f}(x)$  are the reciprocals of the prime factors of  $f(x)$ . If  $f(x)$  is irreducible  $\tilde{f}(x)$  is also irreducible. If  $f(x)$  is primitive  $\tilde{f}(x)$  is also primitive.

Example 2.5: Consider a polynomial  $f(x) = x^3 + x + 1$  over  $GF(2)$ . Its reciprocal polynomial  $\tilde{f}(x)$  is given by

$$\tilde{f}(x) = x^3 \left( \frac{1}{x^3} + \frac{1}{x} + 1 \right) = 1 + x^2 + x^3$$

In this case,  $f(x)$  and  $\tilde{f}(x)$  are both primitive.

Certain Other Useful Properties: Following are certain other useful properties of polynomials over  $GF(p)$ .

- (1) If  $f(x)$  is an irreducible polynomial (other than  $x$ ) of exponent  $e$ , then the exponent of  $[f(x)]^j$  is  $p^r e$  where  $r$  is such that  $p^{r-1} < j \leq p^r$ .
- (2) If  $[f_1(x)]^{k_1}, [f_2(x)]^{k_2}, \dots, [f_r(x)]^{k_r}$  are the prime factors of  $f(x)$  (indivisible by  $x$ ) and if  $e_i$  is the exponent of  $[f_i(x)]^{k_i}$ , then the exponent  $e$  of  $f(x)$  is given by

$$e = \text{LCM}(e_1, e_2, \dots, e_r) \quad (2.4)$$

where LCM stands for least common multiple.

- (3) The prime factors of  $(x - x^p)^k$  are all irreducible polynomials over  $GF(p)$  whose degrees divide  $k$ .
- (4) The polynomial  $(x^{p^m} - 1)$  splits into  $p^m - 1$  linear factors in an extension field  $GF(p^m)$  i.e.

$$(x^{p^m} - 1) = (x - \alpha^0)(x - \alpha^1) \dots (x - \alpha^{p^m-2}) \quad (2.5)$$

Hence all non-zero field elements are various roots of unity.

- (5)  $(1 - x^h)$  divides  $(1 - x^k)$  iff  $h$  divides  $k$ , i.e.  $(1 - x^h)$  is a factor of  $(1 - x^k)$  iff  $h$  is a divisor of  $k$ .

(6) For any polynomial  $f(x)$  over  $GF(p)$ ,

$$[f(x)]^{p^k} = f(x^{p^k}). \quad (2.6)$$

### 2.3 Construction of $GF(p^m)$

We will now see how to construct an extension field  $GF(p^m)$ , starting with the ground field  $GF(p)$ .

Method I: Take the set  $S$  of all polynomials in  $GF(p)$  of degrees less than  $m$ . Define addition between any two elements as normal polynomial addition with the modification that the coefficient of variables now get added according to field addition (i.e. modulo  $p$ ). Define multiplication of any two elements as normal polynomial multiplication, modulo an irreducible polynomial of degree  $m$ . Then the set  $S$  forms  $GF(p^m)$  and satisfies all field axioms. If  $f(x)$  is the irreducible polynomial used, then  $GF(p^m)$  is also denoted by  $E[GF(p); f(x)]$ .

Example 2.6: Consider  $GF(2^2)$  consisting of elements 0, 1,  $x$  and  $1+x$ . The irreducible polynomial used for construction is  $x^2 + x + 1$ . In this addition of two elements say  $x$  and  $x+1$  is given as

$$(x) + (x + 1) = 2x + 1 = 1$$

since  $2 = 0 \pmod{2}$ . Also, their multiplication is given as

$$(x) (x + 1) = x^2 + x = 1 \pmod{x^2 + x + 1}$$

The addition and multiplication tables are given in Table 2.4(a) and Table 2.4(b).

Table 2.4(a) Addition Table  
for  $GF(2^2)$

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$1+x$	0	1
$x+1$	$x+1$	x	1	0

Table 2.4(b) Multiplication  
Table for  $GF(2^2)$

x	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Note that  $GF(2^2)$  of Example 2.3 is isomorphic to this with the mapping  $0 \rightarrow 0$ ,  $1 \rightarrow 1$ ,  $\alpha \rightarrow x$  and  $\alpha^2 \rightarrow x + 1$ .

Method II 13 : Alternatively, we can describe an algorithm for generating elements of  $GF(p^m)$  from  $GF(p)$  as follows. Pick an irreducible polynomial  $p(x)$  of degree  $m$  and coefficients from  $GF(p)$ . Introduce a new symbol  $\alpha$ , and assume  $p(\alpha) = 0$ . Then,  $0, 1, \alpha, \alpha^2, \dots, \alpha^{p^m-2}$  will be a set of  $p^m$  elements of  $GF(p^m)$  such that

$$\alpha^{p^m-1} = 1 \quad (2.7)$$

$$\alpha^i \alpha^j = \alpha^{(i+j) \bmod p^m-1}$$

Example 2.7: Consider the ground field  $GF(2)$ . Let us now construct  $E[(GF(2); x^2 + x + 1)] = GF(2^2)$ . Let  $\alpha$  be an element in  $GF(2^2)$

$$\therefore p(\alpha) = \alpha^2 + \alpha + 1 = 0$$

$$\text{i.e. } \alpha^2 = \alpha + 1$$

Hence the set  $(0, 1, \alpha, \alpha^2)$ , with addition and multiplication as given in Table 2.5(a) and Table 2.5(b), constitute  $GF(2^2)$ .

Table 2.5(a)      Addition Table      Table 2.5(b)      Multiplication  
for  $GF(2^2)$

+	0	1	$\alpha$	$\alpha^2$	x	0	1	$\alpha$	$\alpha^2$
0	0	1	$\alpha$	$\alpha^2$	0	0	0	0	0
1	1	0	$\alpha^2$	$\alpha$	1	0	1	$\alpha$	$\alpha^2$
$\alpha$	$\alpha$	$\alpha^2$	0	1	$\alpha$	0	$\alpha$	$\alpha^2$	1
$\alpha^2$	$\alpha^2$	$\alpha$	1	0	$\alpha^2$	0	$\alpha^2$	1	$\alpha$

Addition and multiplication tables for  $GF(2^3)$ ,  $GF(2^4)$  and  $GF(2^5)$  are given in Appendix A.

#### 2.4 Partial Fraction Expansion of Polynomial Fractions [4]

Let us now see how partial fraction expansion of polynomial fraction over any field can be obtained based on division algorithm. Consider a ratio of two polynomials,

$$\frac{q(x)}{r(x)} = \frac{q(x)}{b_1(x) b_2(x)} \quad (2.8)$$

where  $b_1(x)$  and  $b_2(x)$  are relatively prime. From Equation (2.2) we can write with some  $a_1(x)$  and  $a_2(x)$ ,

$$1 = a_1(x) b_1(x) + a_2(x) b_2(x) . \quad (2.9)$$

Multiplying both sides by  $\frac{q(x)}{r(x)}$ , we get

$$\frac{q(x)}{r(x)} = \frac{a_1(x)}{b_2(x)} q(x) + \frac{a_2(x)}{b_1(x)} q(x) \quad (2.10)$$

In general if  $r(x) = b_1(x) b_2(x) \dots b_r(x)$  where every  $b_i(x)$  and  $b_j(x)$  ( $i \neq j$ ) are relatively prime, we can

$$\frac{q(x)}{r(x)} = \frac{q_1(x)}{b_1(x)} + \frac{q_2(x)}{b_2(x)} + \dots + \frac{q_r(x)}{b_r(x)} \quad (2.11)$$

Now consider the ratio of polynomials

$$\frac{q'(x)}{r'(x)} = \frac{q'(x)}{[b(x)]^k} \quad (2.12)$$

using the division algorithm, the following equations can be successively constructed.

$$q'(x) = f_0(x) b(x) + r_0(x)$$

$$f_0(x) = f_1(x) b(x) + r_1(x)$$

$$f_1(x) = f_2(x) b(x) + r_2(x)$$

⋮

$$f_{k-2}(x) = f_{k-1}(x) b(x) + r_{k-1}(x)$$

where  $\deg r_i(x) < \deg b(x)$ ,  $i = 0, 1, \dots, k-1$ .

By successive substitution we obtain

$$\begin{aligned} q'(x) &= f_0(x) b(x) + r_0(x) \\ &= f_1(x) [b(x)]^2 + r_1(x) b(x) + r_0(x) \\ &= f_2(x) [b(x)]^3 + r_2(x) [b(x)]^2 + r_1(x) b(x) + r_0(x) \\ &= \dots \dots \dots \\ &= f_{k-1} [b(x)]^k + r_{k-1}(x) [b(x)]^{k-1} + \dots + \\ &\quad r_1(x) b(x) + r_0(x) \end{aligned} \quad (2.14)$$

Dividing throughout by  $r'(x)$ , we obtain

$$\frac{q'(x)}{r'(x)} = f_{k-1}(x) + \frac{r_{k-1}(x)}{b(x)} + \frac{r_{k-2}(x)}{[b(x)]^2} + \dots + \frac{r_0(x)}{[b(x)]^k} \quad (2.15)$$

where  $\deg r_i(x) < \deg b(x)$ ,  $i = 0, 1, \dots, k-1$ .

From Equation (2.11) and Equation (2.15) we can state the following. If  $\frac{q(x)}{r(x)}$  is a ratio of two polynomials where

$$r(x) = [p_1(x)]^{k_1} [p_2(x)]^{k_2} \dots [p_r(x)]^{k_r} \quad (2.16)$$

then,  $\frac{q(x)}{r(x)}$  can always be expanded in partial fractions in the form

$$\frac{q(x)}{r(x)} = p(x) + \sum_{i=1}^r \sum_{j=1}^{k_i} \frac{q_{ij}(x)}{[p_i(x)]^j} \quad (2.17)$$

where  $p(x)$  is a polynomial and  $\deg q_{ij}(x) < \deg p_i(x)$ .

Example 2.8: Consider the ratio of two polynomials over GF(2) given by

$$F(x) = \frac{x^5 + x^2 + x}{x^6 + 1}$$

We can write  $x^6 + 1 = (x^3 + 1)^2 = (x + 1)^2 (x^2 + x + 1)^2$

where  $(x + 1)^2$  and  $(x^2 + x + 1)^2$  are relatively prime. Hence from Equation (2.2),

$$1 = a_1(x) (x + 1)^2 + a_2(x) (x^2 + x + 1)^2$$

By inspection,  $a_1(x) = x^2$  and  $a_2(x) = 1$ . This can be obtained by using Euclidean algorithm also, i.e.

$$1 = x^2(x+1)^2 + (x^2 + x + 1)^2$$

Multiplying by  $F(x)$ , we can write

$$F(x) = \frac{x^5 + x^2 + x}{x^6 + 1} = \frac{x^7 + x^4 + x^3}{(x^2 + x + 1)^2} + \frac{x^5 + x^2 + x}{(x+1)^2} \quad (1)$$

Applying division algorithm for the first ratio

$$x^7 + x^4 + x^3 = (1 + x + x^2 + x^3)(1 + x + x^2) + 1$$

$$(1 + x + x^2 + x^3) = (1 + x + x^2)(1 + x + x^2) + x$$

$$\therefore x^7 + x^4 + x^3 = (1 + x + x^2)(1 + x + x^2)^2 + x(1 + x + x^2) + 1$$

Dividing throughout by  $(1 + x + x^2)^2$ , we get

$$\frac{x^7 + x^4 + x^3}{(1 + x + x^2)^2} = 1 + x + x^2 + \frac{x}{(1 + x + x^2)} + \frac{1}{(1 + x + x^2)^2} \quad (2)$$

Now applying division algorithm for the second ratio,

$$x + x^2 + x^5 = (1 + x^2 + x^3 + x^4)(1 + x) + 1$$

$$\text{and } (1 + x^2 + x^3 + x^4) = (1 + x + x^3)(1 + x)$$

$$\therefore (x + x^2 + x^5) = (1 + x + x^3)(1 + x)^2 + 1$$

Dividing by  $(1 + x)^2$ , we obtain

$$\frac{x + x^2 + x^5}{(1 + x)^2} = 1 + x + x^3 + \frac{1}{(1 + x)^2} \quad (3)$$

From Equations (1), (2) and (3) we can write

$$F(x) = \frac{x + x^2 + x^5}{1 + x^6} = \frac{x}{1 + x + x^2} + \frac{1}{(1 + x + x^2)^2} + \frac{1}{(1 + x)^2}$$

## 2.5 Partial Fraction Expansion of Polynomial Fraction Over Galois Fields

Booth [2] suggested a method of achieving partial fraction expansion of polynomial fractions over Galois fields. The method is similar to the one used for polynomial fractions over the field of real and complex numbers.

Consider a polynomial fraction  $F(x)$  as

$$F(x) = x \frac{A(x)}{B(x)} = x \left[ \frac{a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0}{x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0} \right] \quad (2.18)$$

where  $m < n$  and the coefficients  $a_i$  and  $b_i$  are real numbers.

The denominator  $B(x)$  can be factored into the form

$$B(x) = (x - \alpha_1)^{e_1} (x - \alpha_2)^{e_2} \dots (x - \alpha_r)^{e_r} \quad (2.19)$$

where the roots  $\alpha_i$  are either real or complex numbers. The partial fraction expansion of  $F(x)$  then is given by

$$F(x) = x \left[ \frac{k_{1,1}}{(x - \alpha_1)} + \frac{k_{1,2}}{(x - \alpha_1)^2} + \dots + \frac{k_{1,e_1}}{(x - \alpha_1)^{e_1}} + \dots + \frac{k_{r,1}}{(x - \alpha_r)} + \dots + \frac{k_{r,e_r}}{(x - \alpha_r)^{e_r}} \right] \quad (2.19)$$

$$\text{where } k_{i,j} = \frac{1}{(e_i - j)!} \left[ \frac{d^{(e_i - j)}}{dx^{(e_i - j)}} ((x - \alpha_i)^{e_i} \frac{A(x)}{B(x)}) \right] \bigg|_{x = \alpha_i} \quad (2.20)$$

$j = 1, 2, \dots, e_i$

To do a similar thing for polynomial fractions over Galois field, it is required to define a special form of differentiation. In this context, let us see the meaning of the following operation

$$\left[ F(x) \frac{dG(x)}{dx} \right]_{GF(p^n)} ; \quad F(x) \text{ and } G(x) \text{ are over } GF(p^n)$$

It means the following:

1.  $G(x)$  is differentiated, as indicated, but the coefficients of  $G(x)$  are assumed to be arbitrary constants independent of  $x$  and  $GF(p^n)$  while the differentiation operation is taking place.
2. The inside of the brackets is then reduced to simplest form without applying the addition or multiplication properties of  $GF(p^n)$ .
3. After step 2 is completed, the coefficients are reduced by using properties of  $GF(p^n)$ . This operation is called the "formal derivative" of  $G(x)$ .

It is extremely important that the operations are performed in this order.

Example 2.9: As an illustration of the steps mentioned above consider the evaluation of the following expression.

$$\begin{aligned} \left[ \frac{x}{2!} \frac{d^2}{dx^2} \left( \frac{1x}{(x+1)^2} \right) \right]_{GF(2)} &= \left[ \frac{x}{2!} \frac{d}{dx} \left( \frac{(x+1)^2 - x \cdot 2(x+1)}{(x+1)^4} \right) \right]_{GF(2)} \\ &= \left[ \frac{x}{2!} \frac{d}{dx} \left( \frac{(1-x^2)}{(x+1)^4} \right) \right]_{GF(2)} \end{aligned}$$

$$\begin{aligned}
 &= \left[ \frac{x}{2!} \frac{2x-4}{(x+1)^4} \right] \Big|_{GF(2)} \\
 &= \left[ \frac{2x^2-4x}{2! (x+1)^4} \right] \Big|_{GF(2)} = \frac{x^2}{(x+1)^4}
 \end{aligned}$$

Now consider a polynomial fraction  $F(x)$  given by

$$F(x) = \frac{A(x)}{B(x)} = \frac{a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0}{x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0} \quad (2.21)$$

where  $m < r$  and the coefficients  $a_i$  and  $b_i$  are from the field  $GF(p^n)$ . The denominator  $B(x)$  can be written as

$$B(x) = [\mu_1(x)]^{e_1} [\mu_2(x)]^{e_2} \dots [\mu_k(x)]^{e_k} \quad (2.22)$$

where the polynomials  $\mu_i(x)$  are irreducible over  $GF(p^n)$ .

Because the polynomials above can be of any degree, the general partial fraction expansion of  $F(x)$  will have the form

$$\begin{aligned}
 F(x) &= \frac{A_{1,1}(x)}{\mu_1(x)} + \dots + \frac{A_{1,e_1}(x)}{[\mu_1(x)]^{e_1}} + \dots + \frac{A_{k,1}(x)}{\mu_k(x)} \\
 &\quad + \dots + \frac{A_{k,e_k}(x)}{[\mu_k(x)]^{e_k}}
 \end{aligned} \quad (2.23)$$

where  $A_{i,j}(x)$  is a polynomial such that  $\deg A_{i,j}(x) < \deg \mu_i(x)$ .

First assume that  $[\mu_i(x)]^{e_i} = [x - \beta_i]^{e_i}$ , where

$\beta_i \in GF(p^n)$ . Then  $A_{i,j}(x)$  will consist of a single constant term

$$A_{i,j} = \left[ \frac{1}{(e_i-j)!} \frac{d}{dx}^{(e_i-j)} [F(x)(x - \beta_i)^{e_i}] \right]_{GF(p^n)} \Big|_{x=\beta_i} \quad (2.24)$$

where the term inside the brackets indicate the formal derivative of a Galois polynomial.

Next assume that

$$[\mu_i(x)]^{e_i} = [x^k + c_{k-1}x^{k-1} + \dots + c_1x + c_0]^{e_i} \quad (2.25)$$

Then the polynomials  $A_{i,j}(x)$  associated with  $[\mu_i(x)]^j$  in Equation (2.21) are given by

$$A_{i,j}(x) = \left[ \frac{h_j}{(x - u)^j} + \frac{(h_j)^{p^n}}{(x - u^{p^n})^j} + \dots + \frac{(h_j)^{p^{n(k-1)}}}{(x - u^{p^{n(k-1)}})^j} \right] [\mu_i(x)]^j \quad (2.26)$$

where  $u$  is a root of  $\mu_i(x)$  in the extension field  $E[GF(p^n)]$  and

$$h_j = \left[ \frac{1}{(e_i-j)!} \frac{d}{dx}^{(e_i-j)} (F(x)(x-u)^{e_i}) \right]_{E[GF(p^n)]; \mu_i(x)} \Big|_{x=u} \quad (2.27)$$

Example 2.10: Let us consider the same  $F(x)$  as in Example 2.8, i.e.

$$\begin{aligned} F(x) &= \frac{x^5 + x^2 + x}{x^6 + 1} = \frac{x^5 + x^2 + x}{(x + 1)^2(x^2 + x + 1)^2} \\ &= \frac{A_{1,1}}{x + 1} + \frac{A_{1,2}}{(x+1)^2} + \frac{A_{2,1}(x)}{x^2 + x + 1} + \frac{A_{2,2}(x)}{(x^2 + x + 1)^2} \end{aligned}$$

defined over  $GF(2)$ .

We can calculate  $A_{1,1}$  as,

$$\begin{aligned}
 A_{1,1} &= \left[ \frac{d}{dx} F(x)(x+1)^2 \right]_{GF(2)} \Big|_{x=1} \\
 &= \left[ \frac{d}{dx} \frac{x^5 + x^2 + x}{x^6 + 1} (x+1)^2 \right]_{GF(2)} \Big|_{x=1} \\
 &= \left[ \frac{d}{dx} \frac{x^5 + x^2 + k}{(x^2 + x + 1)^2} \right]_{GF(2)} \Big|_{x=1} \\
 &= \frac{x^8 + x^6 + x^2 + 1}{x^8 + x^4 + 1} \Big|_{x=1} = 0
 \end{aligned}$$

and  $A_{1,2}$  as,

$$\begin{aligned}
 A_{1,2} &= \left[ F(x)(x+1)^2 \right] \Big|_{x=1} = \left[ \frac{x^5 + x^2 + x}{x^6 + 1} (x+1)^2 \right] \Big|_{x=1} \\
 &= \frac{x^5 + x^2 + x}{x^4 + x^2 + 1} \Big|_{x=1} = 1
 \end{aligned}$$

To find  $A_{2,1}(x)$  and  $A_{2,2}(x)$  it is necessary to go to the extension field  $E[GF(2); x^2 + x + 1]$  i.e.  $GF(2^2)$ . Using the Table 2.3(a) and Table 2.3(b) we can write,

$$(x^2 + x + 1) = (x + \alpha)(x + \alpha^2)$$

here  $u = \alpha$  and

$$\begin{aligned}
 h_1 &= \left[ \frac{d}{dx} \frac{x^5 + x^2 + x}{x^6 + 1} (x + \alpha)^2 \right]_{GF(2^2)} \Big|_{x=\alpha} \\
 &= \left[ \frac{d}{dx} \frac{x^5 + x^2 + x}{x^4 + \alpha^2 x^2 + \alpha} \right]_{GF(2^2)} \Big|_{x=\alpha}
 \end{aligned}$$

$$= \frac{x^8 + \alpha^2 x^6 + \alpha^2 x^4 + \alpha^2 x^2 + \alpha}{x^8 + \alpha x^4 + \alpha^2} \Big|_{x=\alpha} = \frac{1}{\alpha^2} = \alpha$$

Hence from Equation (2.26)

$$A_{1,1}(x) = \left[ \frac{\alpha}{x+\alpha} + \frac{\alpha^2}{(x+\alpha^2)} \right] (x^2 + x + 1) = \alpha x + \alpha^2 x = x$$

$h_2$  is calculated as,

$$h_2 = \frac{x^5 + x^2 + x}{(x^6 + 1)} (x + \alpha)^2 \Big|_{x=\alpha}$$

$$= \frac{x^5 + x^2 + x}{x^4 + \alpha^2 x^2 + \alpha} \Big|_{x=\alpha} = \frac{\alpha}{\alpha} = 1$$

Therefore from Equation (2.26),  $A_{1,2}(x)$  can be calculated as

$$A_{1,2}(x) = \left[ \frac{1}{(x+\alpha)^2} + \frac{1}{(x+\alpha^2)^2} \right] [x^2 + x + 1]^2 = 1$$

Now we can write

$$F(x) = \frac{x^5 + x^2 + x}{x^6 + 1} = \frac{1}{(x^2 + 1)} + \frac{x}{x^2 + x + 1} + \frac{1}{(x^2 + x + 1)^2}$$

This is same partial fraction expansion as obtained in Example 2.8.

## 2.6 An Useful Result on Polynomials Over GF(p)

We state and prove the following Lemma which will be used in Chapter 3.

**Lemma:** The polynomial  $(1-x^k)$  over GF(p) does not have any  $n^{\text{th}}$  degree primitive polynomial as its factor if  $k \neq aq$  where  $q = p^n - 1$  and  $a$  is some positive integer.

Proof:

Case (i):  $k < q$

Let  $(1-x^k)$  has an  $n^{\text{th}}$  degree primitive polynomial  $f(x)$  as its factor, i.e.  $f(x)$  divides  $1-x^k$  for  $k < q$  which is a contradiction to the definition of primitive polynomial. Hence  $f(x)$  is not a factor.

Case (ii):  $k > q, k \neq aq$

Let

$$(1-x^k) = [f_1(x)]^{k_1} [f_2(x)]^{k_2} \dots [f_j(x)]^{k_j} \quad (2.28)$$

and assume that some of the  $f_i(x)$ 's say  $f_i(x), f_k(x) \dots f_r(x)$  where  $i, k, \dots, r \leq j$ , are primitive and of degree  $n$ . Any such  $[f_i(x)]^{k_i}$  has an exponent  $r'q$  where  $r'$  is such that  $p^{r'-1} < k_i \leq p^{r'}$ . Let

$$p(x) = [f_i(x)]^{k_i} [f_k(x)]^{k_k} \dots [f_r(x)]^{k_r} \quad (2.29)$$

Then the exponent of  $p(x)$  is given by

$$\begin{aligned} e &= \text{LCM}(e_i, e_k, \dots, e_r) \\ &= \text{LCM}(r_i'q, r_k'q, \dots, r_r'q) = r''q \end{aligned} \quad (2.30)$$

Since  $p(x)$  is a factor of  $(1-x^k)$  either  $k = r''q$  or  $k > r''q$ . If  $k > r''q$ ,  $(1-x^k)$  should contain  $(1-x^{r''q})$  as its factor. For this to happen,  $k$  should be equal to some  $r'''(r''q) = aq$  which is a contradiction. Hence we conclude that  $(1-x^k)$  where  $k \neq aq$  does not contain any  $n^{\text{th}}$  degree primitive polynomial as its factor.

## CHAPTER 3

### SCRAMBLER ANALYSIS - INPUT OUTPUT RELATIONS

In Chapter 1, we have discussed that one of the main functions of the scrambler is to map a shorter periodic input sequence into an output sequence of larger periodicity. In this chapter we establish that the scrambler does so in most of the cases. From Section 3.1 to Section 3.5 we develop background material based on D (delay)-transform and M-sequence generator properties. In Section 3.6 we analyse the scrambler for its output periodicity when the period of the input sequence is

- (a) not a multiple of cycle length,
- (b) a multiple of cycle length and
- (c) equal to cycle length:

of the scrambler structure. In Section 3.7 we give specific illustrations to bring out some interesting facts regarding the nature of input sequences of period equal to cycle length and resulting in output sequences of same period irrespective of initial state of the scrambler. Also it is shown that a M-sequence loses its desirable properties due to scrambling, as far as the number of transitions and the cyclic autocorrelation is concerned. In Section 3.8 we discuss complementary partial fraction expansion of the output transform. In Section 3.9 it is shown that the response for linear combination of sequences in the critical state\*, can be obtained by the same linear

---

\* Refer Section 1.8.

combination of the responses due to constituent sequences when the scrambler is in the critical state for these sequences. Also it is shown that the critical state for sequences can be obtained by the same linear combination of the critical states for the constituent sequences.

### 3.1 D-Transform

Consider a sequence  $x(nT)$  such that  $x(t) = 0$  for  $nT < 0$  and taking values only at discrete time intervals. The D-transform of this sequence is defined as

$$D[x(nT)] = x(d) = \sum_{i=0}^{\infty} x_i d^i \quad (3.1)$$

where  $x_i = x(iT)$ ,  $i = 0, 1, \dots$  and  $x_i \in (0, 1)$ .

A finite sequence will have degree of  $d$ , finite. Now consider a sequence  $x(nT)$  to be periodic with period equal to  $q$  (and not any thing less than  $q$ ), i.e.

$$x(nT) = x_0 x_1 \dots x_{q-1} x_0 x_1 \dots x_{q-1} \dots \quad (3.2)$$

Then

$$\begin{aligned} D[x(nT)] &= x(d) = x_0 d^0 + x_1 d^1 + \dots + x_{q-1} d^{q-1} + x_0 d^q + \dots \\ &= (x_0 d^0 + x_1 d^1 + \dots + x_{q-1} d^{q-1})(1 + d^q + d^{2q} + \dots) \end{aligned}$$

i.e.

$$x(d) = \frac{x_0 d^0 + x_1 d^1 + \dots + x_{q-1} d^{q-1}}{1 + d^q} = \frac{x'(d)}{1 + d^q} \quad (3.3)$$

where  $\deg x'(d) \leq q-1$ .

82868

CENTRAL LIBRARY

The inverse D-transform of any  $X(d)$  is the sequence obtained by writing down the coefficients of  $d^i$ ,  $i = 0, 1, 2, \dots$ , in order, i.e.

$$D^{-1}[X(d)] = x(nT) = x_0 x_1 \dots \quad (3.4)$$

Example 3.1: Let  $x(nT) = 010110, 010110, \dots$  Then

$$\begin{aligned} X(d) &= d + d^3 + d^4 + d^7 + d^9 + d^{10} + d^{13} + d^{15} + d^{16} + \dots \\ &= (d + d^3 + d^4)(1 + d^6 + d^{12} + \dots) \end{aligned}$$

i.e.  $X(d) = \frac{d + d^3 + d^4}{1 + d^6}$

Example 3.2: Let  $X(d) = \frac{1 + d^2 + d^3 + d^4}{1 + d^7}$

By long division we can write

$$X(d) = 1 + d^2 + d^3 + d^4 + d^7 + d^9 + d^{10} + d^{11} + \dots$$

i.e.

$$X(d) = (1 + d^2 + d^3 + d^4)(1 + d^7 + d^{14} + d^{21} + \dots)$$

Hence we get

$$x(nT) = 1011100, 1011100, \dots$$

### 3.2 Representation of a Sequence by Polynomial

A sequence  $f(nT)$  can be expressed as a polynomial in  $x$ , where  $x$  is an indeterminate, as follows. Let

$$f(nT) = f_0 f_1 \dots f_r \dots$$

Then, this can be expressed by a polynomial as

$$\begin{aligned}
 f(x) &= f_0 x^0 + f_1 x^1 + \dots + f_r x^r + \dots \\
 &= \sum_{i=0}^{\infty} f_i x^i
 \end{aligned} \tag{3.5}$$

From Equation (3.1) and Equation (3.5) it is clear that the D-transform is nothing but a polynomial representation of the sequence. Hence they are used interchangeably in subsequent sections.

Consider a sequence  $f(nT)$  obtained by bit by bit addition of two sequences  $x(nT)$  and  $y(nT)$  i.e. if

$$x(nT) = x_0 x_1 x_2 \dots$$

$$y(nT) = y_0 y_1 y_2 \dots$$

$$\text{then } f(nT) = x(nT) + y(nT) = f_0 f_1 f_2 \dots$$

$$\text{where } f_i = x_i + y_i, i = 0, 1, 2, \dots$$

The transform of  $f(nT)$  is given by

$$\begin{aligned}
 F(d) &= f_0 d^0 + f_1 d^1 + \dots + f_r d^r + \dots \\
 &= (x_0 + y_0) d^0 + \dots + (x_r + y_r) d^r + \dots \\
 &= x_0 d^0 + x_1 d^1 + \dots + x_r d^r + \dots + \\
 &\quad y_0 d^0 + y_1 d^1 + \dots + y_r d^r + \dots \\
 &= X(d) + Y(d)
 \end{aligned} \tag{3.6}$$

### 3.3 Periodicity of Two Periodic Sequences Added Bit by Bit

Consider two periodic sequences of period s and q, given by

$$y(nT) = y_0 y_1 \dots y_{s-1} y_0 y_1 \dots$$

$$x(nT) = x_0 x_1 \dots x_{q-1} x_0 x_1 \dots$$

Then, bit by bit addition of these two sequences can be structurally represented by shift registers as in Figure 3.1.

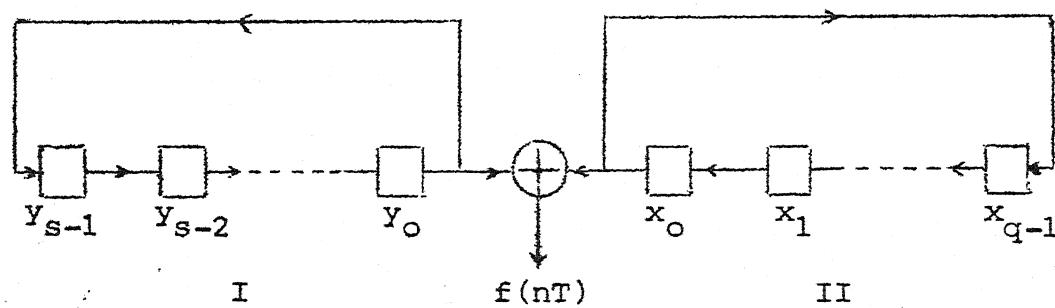


Figure 3.1      Addition of Two Sequences by Shift Registers.

Let  $f(nT)$  be the resultant sequence. Obviously the periodicity of  $f(nT)$  depends on the periodicity of states of the circulating registers. Circulating Register I will be in the same state at any instant  $t = ks$ . Also Register II will be so for any  $t = k'q$ . Hence  $f(nT)$  starts repeating from the instant which satisfies both of these conditions. This instant  $t$  obviously is the LCM of s and q. Hence periodicity of  $f(nT)$  is the LCM of the periods of  $x(nT)$  and  $y(nT)$ .

### 3.4 M-Sequence Generator [9]

Consider a M-sequence generator as shown in Figure 3.2.

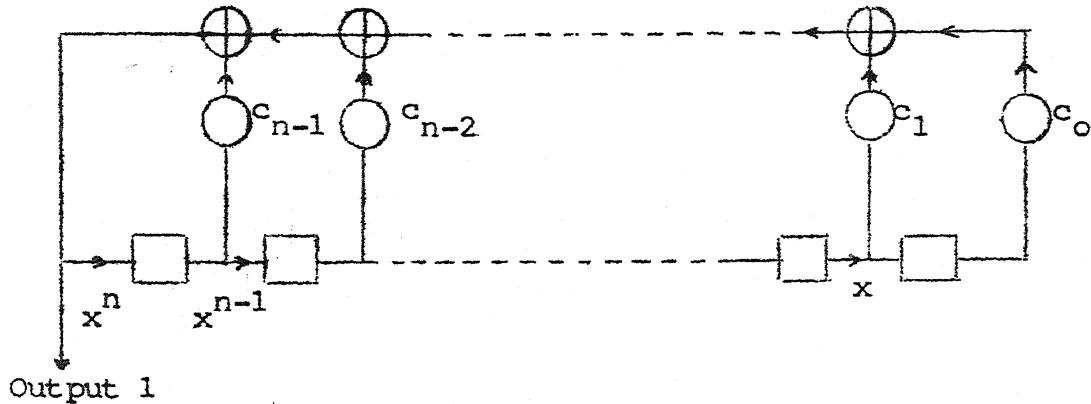


Figure 3.2 M-sequence Generator Structure.

The characteristic equation of the structure is given by

$$c(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x^1 + c_0 \quad (3.7)$$

where  $c_i \in GF(2)$  and  $c(x)$  is a primitive polynomial of  $n^{th}$  degree in  $GF(2)$ .

The  $2^n - 1$  distinct sequences of periodicity  $2^n - 1$  obtained with  $2^n - 1$  distinct non-zero ~~critical~~<sup>initial</sup> states and a sequence of all zeros form a vector space of dimension  $n$ . If these sequences are expressed by polynomials then the least degree polynomial among them is called the generating polynomial  $g(x)$  and is given by

$$g(x) = \frac{x^q + 1}{\tilde{c}(x)} \quad (3.8)$$

where  $q = 2^n - 1$  and  $\tilde{c}(x)$  is the reciprocal polynomial of  $c(x)$ .

The polynomial  $g(x)$  corresponds to a sequence over one period. If we write the sequence as an infinite sequence, then the polynomial corresponding to that is given by

$$\begin{aligned}
 g'(x) &= \frac{x^q + 1}{\tilde{c}(x)} (1 + x^q + x^{2q} + \dots) \\
 &= \frac{x^q + 1}{\tilde{c}(x)} \frac{1}{x^q + 1} = \frac{1}{\tilde{c}(x)}
 \end{aligned} \tag{3.9}$$

### 3.5 Transfer Function of Scrambler

Now consider the following two structures. One scrambler structure and another M-sequence generator with their initial states indicated in Figure 3.3.

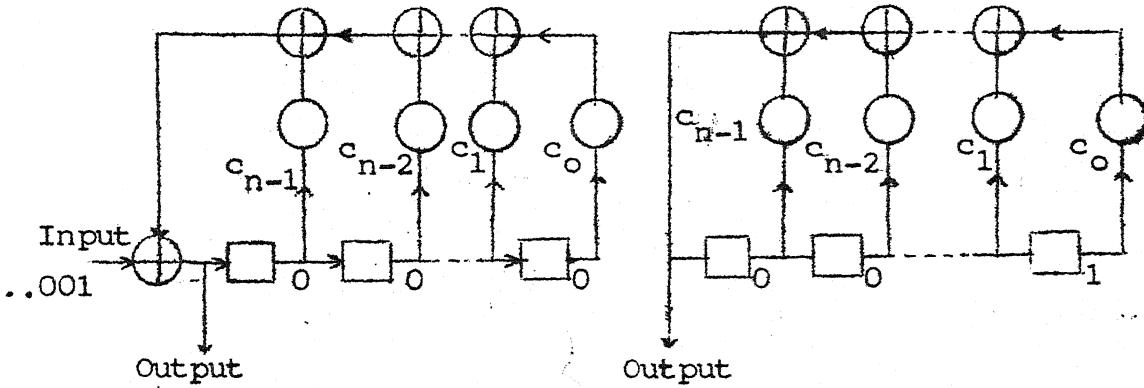


Figure 3.3 Scrambler Structure and M-sequence Generator.

It is clear that the output sequences from the two structures are same; i.e. we can say that the impulse response of the scrambler is nothing but a M-sequence. From the M-sequence structure it can be seen that the M-sequence generated corresponds to the least degree polynomial (over one period), i.e.  $g(x)$ . Hence from Equation (3.9) we can write  $H(d)$ , the transfer function of the scrambler as

$$H(d) = \frac{1}{\tilde{c}(d)} = \frac{(1 + d^q)}{\tilde{c}(d)} \frac{1}{(1 + d^q)} = \frac{q(d)}{1 + d^q} \tag{3.10}$$

where  $\deg q(d) = q = n$ .

Since all M-sequences plus one all zero sequence form a n-dimensional vector space,  $H(d)$ ,  $dH(d)$ , ...,  $d^{n-1}H(d)$  corresponds to n linearly independent sequences of that vector space.

Hence we can write the transform of any M-sequence as

$$p(d) = s(d) H(d) = s(d) \frac{q(d)}{1 + d^q} \quad (3.11)$$

where  $s(d)$  is some polynomial of degree  $\leq n-1$ . Since  $(1+d^q)$  has all the irreducible polynomials except  $d$  of degrees which are divisors of  $n$  as factors, it is clear that  $q(d)$  will have all such factors except  $\tilde{c}(d)$ .

### 3.6 Output Period of Scrambler

Consider the scrambler structure shown in Figure 3.4.

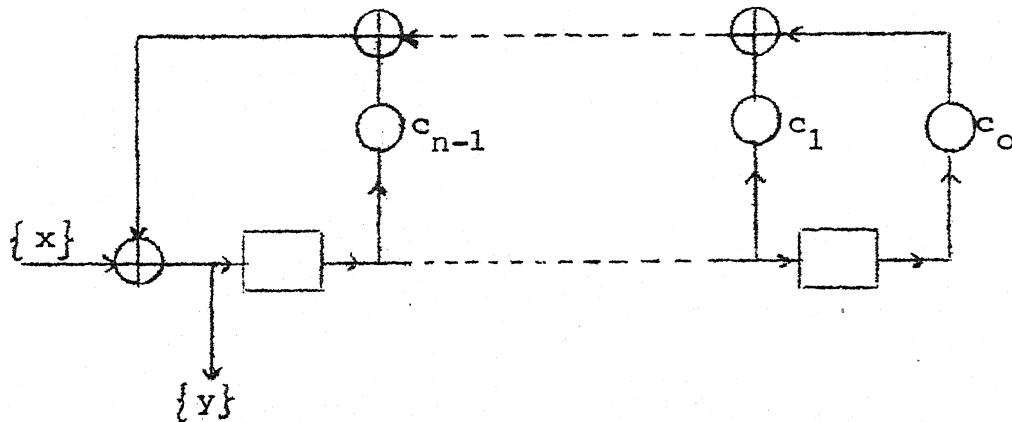


Figure 3.4 Scrambler Structure.

Let  $X(d)$  be the input transform and  $H(d)$  be the transfer function. It can be shown that the system is linear. Hence we can write the output transform  $Y(d)$  as

$$Y(d) = X(d) H(d) \quad (3.12)$$

Now let us study the response of the system to periodic inputs.

Case I: Let the input be of period  $s$  where  $s \neq rq$ ,  $r = 1, 2, \dots$

The input transform be given by

$$X(d) = \frac{p(d)}{1 + d^s}, \quad \deg p(d) \leq s-1 \quad (3.13)$$

$$\text{Then } Y(d) = x(d) H(d)$$

$$= \frac{p(d)}{(1 + d^s)} \frac{q(d)}{(1 + d^q)} = \frac{p(d)}{(1 + d^s) \tilde{c}(d)} \quad (3.14)$$

$$\text{Let } (1 + d^s) = [F_1(d)]^{k_1} [F_2(d)]^{k_2} \dots [F_r(d)]^{k_r} \quad (3.15)$$

From the Lemma proved in Section 2.6, we know that  $\tilde{c}(d)$ , being an  $n^{\text{th}}$  degree primitive polynomial, is not a factor of  $(1 + d^s)$ . Hence, we can write  $Y(d)$  by the partial fraction expansion method as

$$Y(d) = \frac{A_{1,1}(d)}{F_1(d)} + \dots + \frac{A_{1,k_1}(d)}{[F_1(d)]^{k_1}} + \dots + \frac{A_{r,1}(d)}{F_r(d)} + \dots + \frac{A_{r,k_r}(d)}{[F_r(d)]^{k_r}} + \frac{A(d)}{\tilde{c}(d)} \quad (3.16)$$

By combining all terms other than the last one, we can write

$$\begin{aligned} Y(d) &= \frac{p'(d)}{1 + d^s} + \frac{A(d)}{\tilde{c}(d)} \\ &= \frac{p'(d)}{1 + d^s} + \frac{A(d) q(d)}{1 + d^q}, \quad \deg A(d) \leq n-1 \end{aligned} \quad (3.17)$$

This is the output transform, only if the initial state is zero. For non-zero initial states, transform corresponding to

zero input response is to be added to Equation (3.17). Hence from Equation (3.11) we can write  $Y(d)$  as

$$Y(d) = \frac{p'(d)}{1 + d^s} + \frac{A(d) q(d)}{1 + d^q} + \frac{s(d) q(d)}{1 + d^q}, \quad (3.18)$$

where  $\deg A(d), \deg s(d) \leq n-1$ .

$$\text{i.e. } Y(d) = \frac{p'(d)}{1 + d^s} + \frac{q(d)[A(d) + s(d)]}{1 + d^q} \quad (3.19)$$

It can be seen that there will be one particular initial state for which  $A(d) = s(d)$ . In that case,

$$Y(d) = \frac{p'(d)}{1 + d^s} \quad (3.20)$$

i.e. the scrambler is in a critical state for that particular sequence and the output period is  $s$  itself. For other initial states

$$Y(d) = \frac{p'(d)}{1 + d^s} + \frac{q'(d)}{1 + d^q}, \quad \deg q'(d) \leq q-1. \quad (3.21)$$

i.e. the output sequence is of periodicity  $\text{LCM}(s, q)$ .

From Equation (3.20) and Equation (3.21) we can state that if the input sequence to a scrambler is of period  $s$  which is not a multiple of  $(2^n - 1)$ , then the output sequence is of period  $\text{LCM}(s, 2^n - 1)$ , but for a unique initial state for which the output period is  $s$  itself.

Case II: Let  $s = rq$  then,

$$\begin{aligned} Y(d) &= \frac{p(d)}{(1 + d^s)} \frac{q(d)}{(1 + d^q)}, \quad \deg p(d) \leq rq-1, \\ &= \frac{p(d) q(d)}{(1 + d^{rq})(1 + d^q)} \end{aligned} \quad (3.22)$$

(a) If  $p(d)q(d)$  has either  $1+d^{rq}$  or  $1+d^q$  as a factor then  $y(d)$  is given by either

$$Y(d) = \frac{p'(d)}{1+d^q} \quad (3.23)$$

$$\text{or } Y(d) = \frac{p''(d)}{1+d^{rq}} \quad (3.24)$$

i.e. the output period is either  $q$  or  $rq$ .

(b) Let us write  $Y(d)$  as,

$$Y(d) = \frac{p(d)}{(1+d^{rq})} \frac{1}{\tilde{c}(d)} \quad (3.25)$$

Since  $(1+d^q)$  is a factor of  $(1+d^{rq})$ ,  $\tilde{c}(d)$  is definitely a factor of  $1+d^{rq}$ . If  $p(d)$  contains this factor, then there will not be a repeated factor  $\tilde{c}(d)$  in the denominator. In that case, we can write

$$Y(d) = \frac{p'(d)}{1+d^{rq}} + \frac{q'(d)}{1+d^q} \quad (3.26)$$

Therefore the output period =  $\text{LCM}(q, rq) = rq$ .

$$\text{i.e. } Y(d) = \frac{p''(d)}{1+d^{rq}} \quad (3.27)$$

(c) Let us say, after cancellation of common factors if any,

$$Y(d) = \frac{p'(d)}{[F_1(d)]^{k_1} [F_2(d)]^{k_2} \dots [F_r(d)]^{k_r}} \quad (3.28)$$

If we denote the exponent of  $F_i(d)$  by  $e_i$ , then the exponent of  $[F_i(d)]^{k_i}$  is given by  $p^{m_i} e_i$  where  $m_i$  is such that  $p^{m_i-1} < k_i \leq p^{m_i}$  and the exponent of the entire denominator

is given by  $\text{LCM}(p^{m_1}e_1, p^{m_2}e_2, \dots, p^{m_r}e_r)$ . If there is a primitive polynomial (atleast one) of degree  $n$  as a factor, then,

$$\text{LCM}(p^{m_1}e_1, p^{m_2}e_2, \dots, p^{m_r}e_r) = r'q, \quad r' \in (1, 2, \dots),$$

(3.29)

Hence  $Y(d)$  can be written as

$$Y(d) = \frac{p''(d)}{1 + d^{r'q}} \quad (3.30)$$

i.e. the output sequence is of period  $r'q$ .

The cases discussed in (a), (b) and (c) above are all for zero initial state. For non-zero initial states,  $Y(d)$  can be written as,

$$Y(d) = \frac{p''(d)}{1 + d^{r'q}} + \frac{s(d)q(d)}{1 + d^q} \quad (3.31)$$

Hence the output period will be equal to  $\text{LCM}(r'q, q)$ , i.e.  $r'q$  itself.

In Equation (3.28), if none of the  $F_i(d)$ , is a primitive polynomial of degree  $n$ , then the  $\text{LCM}$  of  $(p^{m_1}e_1, p^{m_2}e_2, \dots, p^{m_r}e_r)$  need not be of the kind  $r'q$ . Let us prove that this cannot happen and hence the output period is always some  $r'q$ .

If the exponent of the denominator in Equation (3.28) is some  $q'$ , not a multiple of  $q$ , then

$$Y(d) = \frac{a(d)}{1 + d^{q'}}, \quad \text{where } \deg a(d) \leq q' - n - 1$$

and from Equation (3.12)

$$x(d) = \frac{a(d)}{1 + d^q} \frac{1}{H(d)} = \frac{a(d) \tilde{c}(d)}{1 + d^q}$$

$$\text{i.e. } x(d) = \frac{a'(d)}{1 + d^q}, \quad \deg a'(d) \leq q - 1 \quad (3.32)$$

This contradicts our assumption that the input period  $s$  is equal to  $rq$ .

We can state that when the input is of period  $rq$ , the output period will be some  $r'q$ , irrespective of the initial state.

Case III: Let  $s = q$

Though this is covered in Case II, let us consider separately the case of input period equal to  $q$ , i.e. let

$$x(d) = \frac{p(d)}{1 + d^q}, \quad \deg p(d) \leq q - 1$$

$$\text{Then } y(d) = x(d) H(d) = \frac{p(d)}{1 + d^q} \frac{1}{\tilde{c}(d)} = \frac{p(d)}{1 + d^q} \frac{q(d)}{1 + d^q} \quad (3.33)$$

If  $p(d) q(d)$  has a factor  $(1 + d^q)$ , then the periodicity of the output will be  $q$ . If  $p(d) q(d)$  does not have  $(1 + d^q)$  as a factor, then the output period will be equal to  $2q$ . Let us say  $p(d) q(d)$  has  $(1 + d^q)$  as a factor i.e.

$$p(d) q(d) = r(d) (1 + d^q)$$

$$p(d) = \frac{(1 + d^q) r(d)}{q(d)} = \tilde{c}(d) r(d) \quad (3.34)$$

where  $\deg p(d) \leq q - 1$ ;  $\deg \tilde{c}(d) = n$ . Therefore,

$$\deg r(d) \leq q - (n + 1) = 2^n - n - 2$$

Hence there are  $(2^{(2^n-n-1)} - 2)$  sequences of period  $q$ , which gives rise to output period of  $q$  itself (excluding all zeros' and all ones' sequences).

Substituting for  $p(d)$  in Equation (3.33)

$$Y(d) = \frac{\tilde{c}(d) r(d)}{1 + d^q} \cdot \frac{1}{\tilde{c}(d)} = \frac{r(d)}{1 + d^q} \quad (3.35)$$

If the initial state is non-zero, then

$$\begin{aligned} Y(d) &= \frac{r(d)}{1 + d^q} + \frac{s(d) q(d)}{1 + d^q} \\ &= \frac{r'(d)}{1 + d^q}, \quad \deg r'(d) \leq q - 1 \end{aligned} \quad (3.36)$$

i.e. the output period is  $q$ , irrespective of the initial state for these  $(2^{(2^n-n-1)} - 2)$  sequences except when  $p(d)$  corresponds to a sequence with internal periodicity. For these cases if we write  $p(d)$  as

$$p(d) = (p_{q-1}d^{q-1} + p_{q-2}d^{q-2} + \dots + p_1d + p_0) \quad (3.37)$$

then it can have periodicities of period  $i$ , for all  $i$ 's which are non-trivial divisors of  $q$ . The total number  $N$  of such sequences is given by

$$N = \sum_{\substack{i \\ i|q \\ i \neq q}} (2^i - 2) \quad (3.38)$$

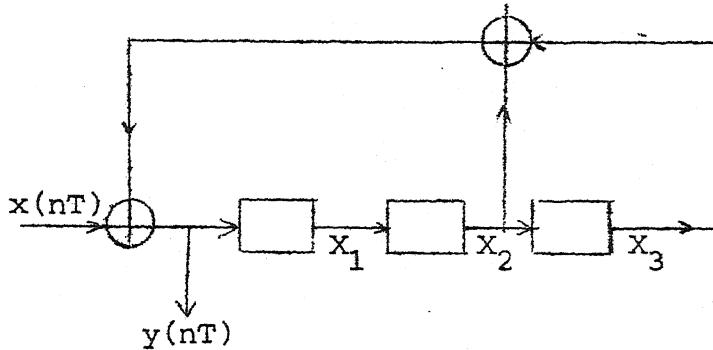
These sequences will give rise to period  $i$  itself when scrambler is in critical state, with this, we can state the following.

For a scrambler of cycle length  $q$  where  $q = 2^n - 1$ , there are exactly  $N'$  number of input sequences of period  $q$ .

which results in output sequences of period  $q$  itself irrespective of initial state, where  $N'$  is given by

$$N' = 2^{(2^n - n - 1)} - 2 - \sum_{\substack{i \\ i|q \\ i \neq q}} (2^i - 2) \quad (3.39)$$

Example 3.3: Consider a scrambler structure of characteristic polynomial  $c(x) = x^3 + x + 1$



Scrambler Structure for Example 3.3.

Impulse response is, 1011100,1011100 ...

$$\therefore H(d) = \frac{1 + d^2 + d^3 + d^4}{1 + d^7}$$

The zero input response and their transform for various non-zero initial states are given in Table 3.1

Let the input transform be given by

$$X(d) = \frac{d^2 + d}{1 + d^3}$$

$$\text{then } Y(d) = X(d) H(d) = \frac{d^2 + d}{1 + d^3} \cdot \frac{1 + d^2 + d^3 + d^4}{1 + d^7}$$

$$\text{i.e. } Y(d) = \frac{d^2}{(d^2 + d + 1)(d^3 + d^2 + 1)}$$

Table 3.1 Zero Input Response and Their Transform

Initial State			Response	Transform
$x_1$	$x_2$	$x_3$		
0	0	1	1011100,10 ...	$H(d)$
0	1	0	1110010,11 ...	$(1 + d)H(d)$
0	1	1	0101110,01 ...	$d H(d)$
1	0	0	0111001,01 ...	$(d + d^2)H(d)$
1	0	1	1100101,11 ...	$(1 + d + d^2)H(d)$
1	1	0	1001011,10 ...	$(1 + d^2)H(d)$
1	1	1	0010111,00	$d^2 H(d)$

From Section 2.5, we can write this as

$$Y(d) = \frac{A_{1,1}(d)}{d^2 + d + 1} + \frac{A_{2,1}(d)}{d^3 + d^2 + 1} \quad (1)$$

where

$$A_{1,1}(d) = \frac{h_1}{(d + \alpha)} + \frac{h_1^2}{d + \alpha^2} (d^2 + d + 1), \quad (2)$$

is a root of  $d^2 + d + 1 = 0$  in  $E[GF(2); d^2 + d + 1]$ ,

$$h_1 = \left[ \frac{d}{(d^2 + d + 1)(d^3 + d^2 + 1)} \cdot (d + \alpha) \right]_{GF(2^2)} \Big|_{d = \alpha}, \quad (3)$$

$$\text{and } A_{2,1}(d) = \left[ \frac{h_2}{(d + \beta)} + \frac{h_2^2}{(d + \beta^2)} + \frac{h_2^4}{(d + \beta^4)} \right] (d^3 + d^2 + 1) \quad (4)$$

is a root of  $d^3 + d^2 + 1 = 0$  in  $E[GF(2); d^3 + d^2 + 1]$

$$h_2 = \left[ \frac{d}{(d^2 + d + 1)(d^3 + d^2 + 1)} \cdot (d + \beta) \right]_{GF(2^3)} \Big|_{d=\beta} \quad (5)$$

Now let us calculate  $A_{1,1}(d)$  and  $A_{2,1}(d)$ . From Equation (3) and referring to Table 2.5(a) and Table 2.5(b),

$$\begin{aligned} h_1 &= \left[ \frac{d}{(d + \alpha^2)(d^3 + d^2 + 1)} \right]_{GF(2^2)} \Big|_{d=\alpha} \\ &= \frac{d}{d^4 + \alpha d^3 + \alpha^2 d^2 + \alpha + \alpha^2} \Big|_{d=\alpha} = \alpha^2 \end{aligned} \quad (6)$$

From Equation (2),

$$A_{1,1}(d) = \frac{\alpha^2}{d + \alpha} + \frac{\alpha}{d + \alpha^2} (d^2 + d + 1) = d + 1 \quad (7)$$

From Equation (5) and referring to tables of  $E[GF(2^3); d^3 + d^2 + 1]$  in Appendix A

$$h_2 = \left[ \frac{d}{(d^2 + d + 1)(d + \beta^2)(d + \beta^4)} \right]_{GF(2^3)} \Big|_{d=\beta}$$

Since  $d^3 + d^2 + 1 = (d + \beta)(d + \beta^2)(d + \beta^4)$ .

$$h_2 = \frac{d}{d^4 + \beta d^3 + \beta^2 d^2 + \beta^3 d + \beta^6} \Big|_{d=\beta} = \beta^2 \quad (8)$$

Therefore from Equation (4),

$$A_{2,1}(d) = \frac{\beta^2}{d + \beta} + \frac{\beta^4}{d + \beta^2} + \frac{\beta}{d + \beta^4} = d^2 + d + 1 \quad (9)$$

Hence we can write  $Y(d)$  as

$$\begin{aligned}
 Y(d) &= \frac{d+1}{d^2+d+1} + \frac{d^2+d+1}{(d^3+d^2+1)} \\
 &= \frac{1+d^2}{1+d^3} + \frac{(d^2+d+1)(1+d)(1+d+d^3)}{1+d^7}
 \end{aligned}$$

$$\text{i.e. } Y(d) = \frac{1+d^2}{1+d^3} + (d^2+d+1) H(d),$$

for zero initial state. From Table 3.1 we can see that for initial state 1 0 1,

$$Y(d) = \frac{1+d^2}{1+d^3} + (d^2+d+1) H(d) + (d^2+d+1) H(d)$$

i.e. the output period is 3 itself and the output sequence  $y(nT)$  is, 101,101,...

For any other initial state,

$$Y(d) = \frac{1+d^2}{1+d^3} + \frac{s(d)(1+d^2+d^3+d^4)}{1+d^7}, \quad \deg s(d) \leq 2$$

Hence output period is  $\text{LCM}(3,7) = 21$ .

Example 3.4: For the same structure as in Example 3.3, let

$$\begin{aligned}
 X(d) &= \frac{1+d+d^3+d^4+d^5+d^6+d^9}{1+d^{21}} \\
 &= \frac{(1+d^2+d^3)^2 (d^3+d+1)}{1+d^{21}}
 \end{aligned}$$

We have  $Y(d) = X(d) H(d)$

$$= \frac{(1+d^2+d^3)^2 (d^3+d+1)}{1+d^{21}} \cdot \frac{1}{d^3+d^2+1}$$

$$\text{i.e. } Y(d) = \frac{(1+d^2+d^3)(d^3+d+1)}{1+d^{21}}$$

$$= \frac{1}{(1+d)(d^2+d+1)(d^6+d^4+d^2+d+1)(d^6+d^5+d^4+d^2+1)}$$

Here,  $(1+d)$  is of exponent 1

$d^2+d+1$  is of exponent 3

$d^6+d^4+d^2+d+1$  is of exponent 21

$d^6+d^5+d^4+d^2+1$  is of exponent 21

Hence exponent of denominator is  $\text{LCM}(1, 3, 21, 21) = 21$  and we can write

$$\begin{aligned} y(d) &= \frac{(d^3+d^2+1)(d^3+d+1)}{1+d^{21}} \\ &= \frac{d^6+d^5+d^4+d^3+d^2+d+1}{1+d^{21}} \end{aligned}$$

i.e. the output period is 21 and the output sequence  $y(nT)$  is,

1111111000000000000000000,111 ...

### 3.7 Specific Illustrations

Based on the general analysis we will now consider the behaviour of scrambler with specific structure and/or specific input.

(1) Consider a three stage scrambler. From Equation (3.38),

$$N' = 2^{(8-3-1)} - 2 = 14, \text{ since } \sum_{\substack{i=1 \\ i \neq 7}}^7 2^i - 2 = 0$$

i.e. there are 14 distinct sequences of period 7 which results in output sequences of period 7 itself.

Now consider a M-sequence generated with  $\tilde{C}(x) -$  the reciprocal polynomial of scrambler structure as the characteristic

polynomial. Say,  $\tilde{c}(x) = x^3 + x^2 + 1$ . Then, any M-sequence generated by it will have the transform

$$x(d) = \frac{r'(d)(1+d)(d^3 + d^2 + 1)}{1+d^7}, \quad \deg r'(d) \leq 2 \quad (3.40)$$

Let this be given as input to the scrambler structure with characteristic polynomial  $c(x) = x^3 + x + 1$ . Then,

$$\begin{aligned} y(d) &= x(d) H(d) \\ &= \frac{r'(d)(1+d)(d^3 + d^2 + 1)}{1+d^7} \cdot \frac{(1+d)(d^3 + d + 1)}{(1+d^7)} \\ y(d) &= \frac{r'(d)(1+d)}{1+d^7} \end{aligned} \quad (3.41)$$

For non-zero initial states

$$\begin{aligned} y(d) &= \frac{r'(d)(1+d)}{1+d^s} + \frac{s'(d)(1+d)(1+d+d^3)}{1+d^q}, \\ &\quad \deg s'(d) \leq 2 \end{aligned} \quad (3.42)$$

$$\text{i.e. } y(d) = \frac{r''(d)}{1+d^7}, \quad \deg r''(d) \leq 6 \quad (3.43)$$

Therefore the output period is 7, independent of the initial state. Obviously the complements\* of these seven sequences also give rise to output period equal to 7; i.e. there are 14 such sequences. Hence for three stage scramblers, we can state that only M-sequences generated by the reciprocal structure (with respect to scrambler structure) and their complements give rise to output sequence of period 7.

\* A sequence complement to  $x(nT)$  is given by

$$\bar{x}(nT) = \bar{x}_0 \bar{x}_1 \bar{x}_2 \dots$$

(2) In the case of 4 stage scrambler from Equation (3.32),

$$N' = 2^{(2^4-4-1)} - 2 - \sum_{\substack{i=1 \\ i \mid 15 \\ i \neq 15}} (2^i - 2) = 2010$$

Now consider a M-sequence generated with  $\tilde{c}(x)$  - the reciprocal polynomial of scrambler structure - as the characteristic polynomial; say  $\tilde{c}(x) = x^4 + x^3 + 1$ . Then, from Section 3.5 any M-sequence generated by it will have the transform,

$$x(d) = \frac{r'(d)(1+d)(1+d+d^2)(1+d+d^2+d^3+d^4)(1+d^3+d^4)}{1+d^{15}}$$

$$\deg r'(d) \leq 3 \quad (3.44)$$

Let this be given as input to the scrambler structure with characteristic polynomial  $c(x) = x^4 + x + 1 = 0$ . From Section 3.5 the transfer function  $H(d)$  is given by

$$H(d) = \frac{(1+d)(1+d+d^2)(1+d+d^2+d^3+d^4)(1+d+d^4)}{1+d^{15}}$$

$$\therefore y(d) = \frac{r'(d)(1+d)(1+d+d^2)(1+d+d^2+d^3+d^4)}{1+d^{15}}$$

For non-zero initial states,

$$y(d) = \frac{r'(d)(1+d)(1+d+d^2)(1+d+d^2+d^3+d^4)}{1+d^{15}}$$

$$+ \frac{s'(d)(1+d)(1+d+d^2)(1+d+d^2+d^3+d^4)(1+d+d^4)}{1+d^{15}},$$

$$\deg s'(d) \leq 3 \quad (3.45)$$

$$= \frac{r''(d)}{1+d^{15}}, \quad \deg r''(d) \leq 14 \quad (3.46)$$

i.e. the output period is 15 independent of the initial state. There are 15 such M-sequences. Obviously, sequences complement to these sequences also give rise to output sequences of period 15, irrespective of the initial state.

(3) Now consider a scrambler structure of  $n$  stages in general with a characteristic polynomial  $c(x)$ . Then, the transfer function  $H(d)$  is given by

$$H(d) = \frac{1}{\tilde{c}(d)} \quad (3.47)$$

If the output of any other M-sequence structure of degree  $n$  with characteristic polynomial  $c'(x)$  is given as input to the scrambler, then from Section 3.5 we can write the input transform as,

$$X(d) = \frac{s(d)}{\tilde{c}'(d)}, \quad \deg s(d) \leq n - 1 \quad (3.48)$$

Therefore output transform is given by

$$Y(d) = \frac{s(d)}{\tilde{c}'(d) \tilde{c}(d)} \quad (3.49)$$

Here  $\tilde{c}'(d)$  and  $\tilde{c}(d)$  are two different primitive polynomials of degree  $n$ . Hence  $Y(d)$  can be written as

$$Y(d) = \frac{s'(d)}{1 + d^q}, \quad q - 2n \leq \deg s'(d) \leq q - n - 1 \quad (3.50)$$

For non-zero initial states, from Section 3.5 we can write

$$Y(d) = \frac{s'(d)}{1 + d^q} + \frac{r(d)}{1 + d^q}, \quad q - n \leq \deg r(d) \leq q - 1 \quad (3.51)$$

$$\text{i.e. } Y(d) = \frac{s''(d)}{1 + d^q}, \quad q - 2n \leq \deg s''(d) \leq q - 1 \quad (3.52)$$

The output period is  $q$  independent of initial state. It follows that this is so when the input is any sequence complement to these input sequences. Therefore we can state that for a scrambler of  $M$  stages with characteristic polynomial  $c(x)$ . If the sequences generated by any  $M$ -sequence generator of the same number of stages and characteristic polynomial other than  $c(x)$  or the complement of these sequences are given as input, then the output period will be equal to  $q$ , the cycle length.

The observation made with respect to 3 and 4 stage scramblers respectively in Illustration 2 and Illustration 4, is covered in this general statement.

(4) We have seen that there is no advantage in scrambling a  $M$ -sequence of period  $q$ , as far as its periodicity is concerned, except when the sequence is one of the sequences generated by the same structure as that of the scrambler. The next question is whether other desirable characteristics of a  $M$ -sequence, say number of transitions and cyclic autocorrelation function (CACF) are still retained at the output.

Consider the three stage scrambler with characteristic polynomial  $c(x) = x^3 + x + 1$ , with input, a  $M$ -sequence generated by the structure with characteristic polynomial  $\tilde{c}(x) = x^3 + x^2 + 1$ . Then Equation (3.42) gives the output transform  $Y(d)$  for non-zero initial states as

$$\begin{aligned}
 Y(d) &= \frac{r'(d)(1+d)}{1+d^7} + \frac{s'(d)(1+d)(1+d+d^3)}{1+d^7} \\
 &= \frac{(1+d)[r'(d) + s'(d)(1+d+d^3)]}{1+d^7} \quad (3.53)
 \end{aligned}$$

$\deg r'(d), \deg s'(d) \leq 2$

For a given  $r'(d)$  there can be solutions to  $s'(d)$  such that the numerator say,  $p'(d)$  is of the kind

$$p'(d) = d^l + d^{l+1} + \dots + d^{l+m} \quad (3.54)$$

where  $l \in (0, 1, \dots, 6)$ ,  $m \in (0, 1, \dots, 5)$  and  $\oplus$  is addition modulo 7.

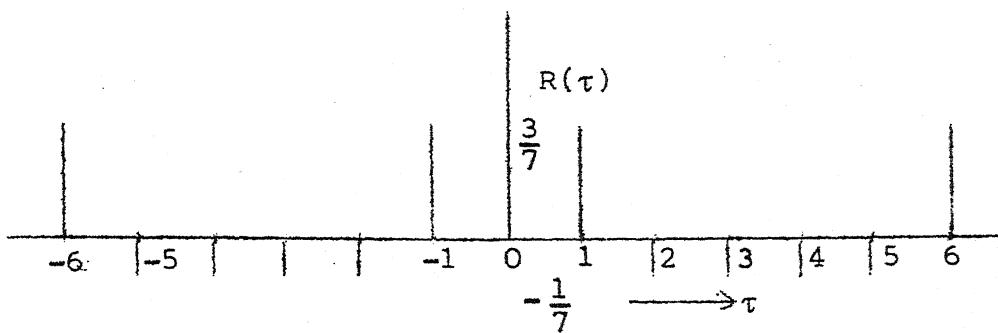
In that case,  $Y(d)$  corresponds to an output sequence which has only two transitions over one period. All such combinations of  $r'(d)$  and  $s'(d)$  and  $p'(d)$  resulting in these cases are listed in Table 3.2. It can be seen that there are three classes of output sequences having minimum number of transitions, i.e. 2. Obviously the CACF of all sequences in a class is same. The CACFs for these three classes are shown in Figure 3.5. It is seen that the ideal CACF of a M-sequence is lost due to scrambling.

It is verified exhaustively in the case of 3, 4 and 5 stage scramblers that the ideal CACF of a M-sequence in almost all the cases, is lost due to scrambling. In most of the cases the number of transitions in the output sequence is less than that in the input M-sequence. Only in a very few cases they are more than that in the input M-sequence. The minimum number of transitions observed for four stage scramblers is 4.

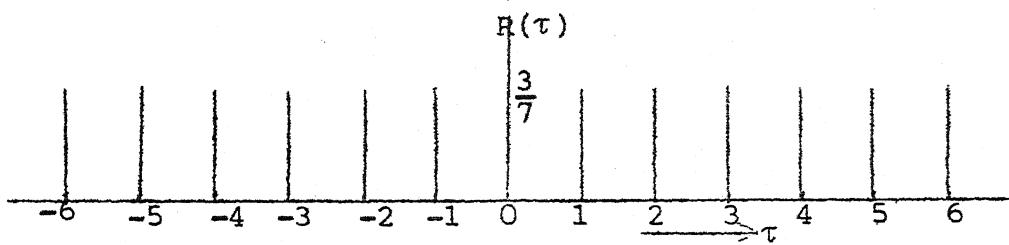
(5) Now let us consider another interesting question, i.e. whether it is possible to get a M-sequence at the output of a scrambler in a situation discussed in the previous illustration. Let  $c(x)$  be the characteristic polynomial of a  $n$  stage scrambler. Consider a M-sequence generated by a  $n$  stage M-sequence generator with the characteristic polynomial  $c'(x)$ , as the input. Proceeding exactly the

Table 3.2 Cases of Minimum Number of Transitions

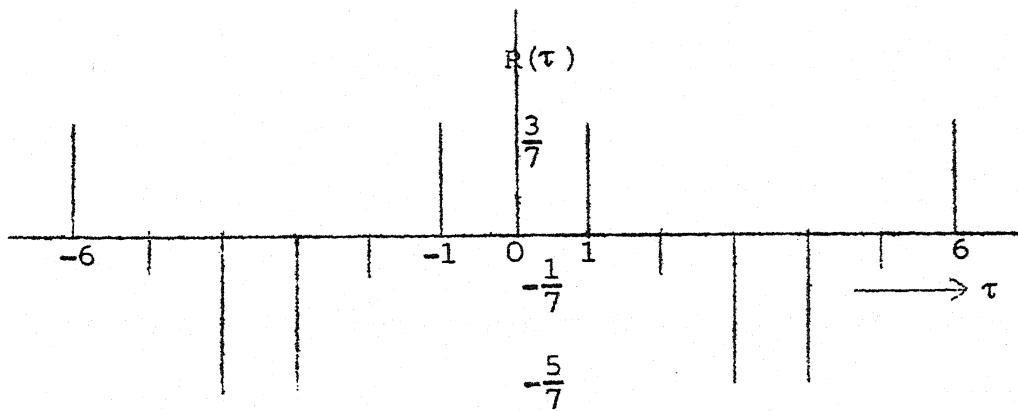
$r^*(d)$	$s^*(d)$	$p^*(d)$
1	1	$d + d^2 + d^3 + d^4$
	$d^2$	$1 + d + d^2 + d^4 + d^5 + d^6$
$d$	$d$	$d^2 + d^3 + d^4 + d^5$
	$1 + d^2$	$1 + d + d^2 + d^3 + d^5 + d^6$
$d^2$	$d^2$	$d^3 + d^4 + d^5 + d^6$
	$1 + d + d^2$	$1 + d + d^2 + d^3 + d^4 + d^6$
$1 + d$	1	$d^3 + d^4$
	$d$	$1 + d + d^2 + d^3 + d^4 + d^5$
	$d^2$	$1 + d^4 + d^5 + d^6$
$1 + d^2$	$d^2$	$1 + d + d^3 + d^4 + d^5 + d^6$
	$d^2 + d$	$1 + d^6$
$d + d^2$	$d$	$d^4 + d^5$
	$d^2$	$d + d^2 + d^3 + d^4 + d^5 + d^6$
	$1 + d^2$	$1 + d + d^2 + d^3 + d^5 + d^6$
$1 + d + d^2$	$d^2$	$1 + d^2 + d^3 + d^4 + d^5 + d^6$
	$1 + d^2$	$d^5 + d^6$
	$d + d^2$	$1 + d + d^2 + d^6$



(i) CACF for  $p'(d) = d^3 + d^4$ .



(ii) CACF for  $p'(d) = 1 + d + d^2 + d^3 + d^4 + d^5$ .



(iii) CACF for  $p'(d) = d + d^2 + d^3 + d^4$ .

Figure 3.5 CACFs of Scrambled M-sequence.

same way as we did for obtaining Equation (3.44), the output transform for any initial state can be written as

$$\begin{aligned}
 Y(d) &= \frac{r(d) p(d) + s(d) p(d) c(d)}{1 + d^q}, \\
 &= \frac{p(d) [r(d) + s(d) c(d)]}{1 + d^q}, \quad \deg r(d), \deg s(d) \leq n-1
 \end{aligned} \tag{3.55}$$

$$\text{where } p(d) = \frac{1 + d^q}{c(d) c'(d)} \tag{3.56}$$

This  $Y(d)$  can correspond to a M-sequence of length  $q$  only under the following conditions.

$$(1) \quad r(d) + s(d) c(d) = r'(d) c(d), \quad \deg r'(d) \leq n-1$$

$$(2) \quad r(d) + s(d) c(d) = r''(d) c'(d), \quad \deg r''(d) \leq n-1$$

It is obvious that the first condition can be satisfied only when  $r(d) = 0$  and in that case  $r'(d) = s(d)$  and the output is nothing but the zero input response of a scrambler, a M-sequence. This is a trivial solution. There can be solutions to  $s(d)$  for a given  $r(d)$  such that the condition 2 is satisfied and in that case it is evident that the scrambler acts just as a delay element. Such cases for 3, 4 and 5 stage scramblers are listed in Table 3.3. In all cases there is only one solution to  $s(d)$ .

### 3.8 Complementary Partial Fraction Expansion

Let us now see whether the partial fraction expansion of the output transform we have used in this chapter is unique. After cancellation of terms let  $Y(d)$  be given by

Table 3.3 Cases where Scrutinizer Provides Details for Specific Items

(cont'd.)

Table 3.3 contd.

input/scrambler Structure	Initial State	input M-Sequence / Delay
9/8	01000	...../5
9/10	00110	...../22
10/5	10110	1000010110101001101111001001/20
10/6	11101	...../8
10/7	01101	...../21
10/8	10111	...../10
10/9	00111	...../3

Polynomials are numbered as follows:

1.  $x^3 + x^2 + 1$
2.  $x^3 + x + 1$
3.  $x^4 + x^3 + 1$
4.  $x^4 + x^2 + 1$
5.  $x^5 + x^2 + 1$
6.  $x^5 + x^3 + 1$
7.  $x^5 + x^4 + x^3 + x + 1$
8.  $x^5 + x^4 + x^2 + x + 1$
9.  $x^5 + x^4 + x^3 + x^2 + x + 1$
10.  $x^5 + x^3 + x^2 + x + 1$

$$Y(d) = \frac{A(d)}{[F_1(d)]^{k_1} [F_2(d)]^{k_2} \cdots [F_r(d)]^{k_r}} \quad (3.57)$$

The partial fraction expansion of  $Y(d)$  be

$$Y(d) = \frac{A_{1,1}(d)}{F_1(d)} + \cdots + \frac{A_{1,k_1}(d)}{[F_1(d)]^{k_1}} + \cdots + \frac{A_{r,1}(d)}{F_r(d)} + \cdots + \frac{A_{r,k_r}(d)}{[F_r(d)]^{k_r}} \quad (3.58)$$

where  $\deg A_{i,j}(d) < \deg F_i(d)$

If the exponent of  $[F_i(d)]^{k_i}$  is denoted by  $e_{i,k_i}$  then we can write  $Y(d)$  as

$$Y(d) = \frac{B_{1,1}(d)}{1 + d^{e_{1,1}}} + \cdots + \frac{B_{1,k_1}(d)}{1 + d^{e_{1,k_1}}} + \cdots + \frac{B_{r,1}(d)}{1 + d^{e_{r,1}}} + \cdots + \frac{B_{r,k_r}(d)}{1 + d^{e_{r,k_r}}}, \quad \deg B_{i,j}(d) = e_{i,j} - 1 \quad (3.59)$$

Let  $R(d)$  be another polynomial fraction given by

$$R(d) = \frac{\bar{B}_{1,1}(d)}{1 + d^{e_{1,1}}} + \cdots + \frac{\bar{B}_{1,k_1}(d)}{1 + d^{e_{1,k_1}}} + \cdots + \frac{\bar{B}_{r,1}(d)}{1 + d^{e_{r,1}}} + \cdots + \frac{\bar{B}_{r,k_r}(d)}{1 + d^{e_{r,k_r}}} \quad (3.60)$$

where  $\deg \bar{B}_{i,j}(d) \leq e_{i,j} - 1$  and  $\bar{A}(d)$  is defined by

$$\bar{A}(d) = \bar{a}_0 + \bar{a}_1 d + \cdots + \bar{a}_{q-1} d^{q-1}$$

if  $A(d) = a_0 + a_1 d + \cdots + a_{q-1} d^{q-1}$  (3.61)

Their sum is given by

$$\begin{aligned}\bar{A}(d) + A(d) &= (\bar{a}_0 + a_0) + (\bar{a}_1 + a_1)d + \dots + (\bar{a}_{q-1} + a_{q-1})d^{q-1} \\ &= 1 + d + \dots + d^{q-1}\end{aligned}\quad (3.62)$$

Adding Equation (3.59) and Equation (3.60)

$$\begin{aligned}Y(d) + R(d) &= \frac{[B_{1,1}(d) + \bar{B}_{1,1}(d)]}{1 + d^{e_{1,1}}} + \dots + \frac{[B_{1,k_1}(d) + \bar{B}_{1,k_1}(d)]}{1 + d^{e_{1,k_1}}} \\ &\quad + \dots + \frac{[B_{r,1}(d) + \bar{B}_{r,1}(d)]}{1 + d^{e_{r,1}}} \\ &\quad + \dots + \frac{[B_{r,k_r}(d) + \bar{B}_{r,k_r}(d)]}{1 + d^{e_{r,k_r}}} \\ &= \frac{1}{1 + d} + \frac{1}{1 + d} + \dots, \quad j = \sum_{j=1}^r k_j \text{ times}\end{aligned}\quad (3.63)$$

Now if  $j$  is even, then

$$Y(d) + R(d) = 0, \text{ i.e. } Y(d) = R(d). \text{ Therefore}$$

$$\begin{aligned}Y(d) &= \frac{\bar{B}_{1,1}(d)}{1 + d^{e_{1,1}}} + \dots + \frac{\bar{B}_{1,k_1}(d)}{1 + d^{e_{1,k_1}}} + \dots + \frac{\bar{B}_{r,1}(d)}{1 + d^{e_{r,1}}} \\ &\quad + \dots + \frac{\bar{B}_{r,k_r}(d)}{1 + d^{e_{r,k_r}}}\end{aligned}\quad (3.64)$$

is also a solution if  $j$  is even. Now consider Equation (3.17)

i.e.

$$Y(d) = \frac{p'(d)}{1 + d^s} + \frac{A(d) q(d)}{1 + d^q} = \frac{p'(d)}{1 + d^s} + \frac{q'(d)}{1 + d^q}$$

where  $\deg A(d) \leq n-1$ ,  $\deg q(d) \leq q-1$ .

From Equation (3.64) it follows that  $Y(d)$  can also be written as

$$Y(d) = \frac{\bar{p}'(d)}{1 + d^s} + \frac{\bar{q}'(d)}{1 + d^q}, \quad \deg q'(d) \leq q - 1 \quad (3.65)$$

For non-zero initial state,  $Y(d)$  is given by

$$Y(d) = \frac{\bar{p}'(d)}{1 + d^s} + \frac{\bar{q}'(d)}{1 + d^q} + \frac{s(d) q(d)}{1 + d^q}, \quad \deg s(d) \leq n-1 \quad (3.66)$$

In this case, for a particular initial state

$$\frac{\bar{q}'(d)}{1 + d^q} + \frac{s(d) q(d)}{1 + d^q} = \frac{1}{1 + d} \quad (3.67)$$

i.e. it corresponds to a sequence of all ones. Hence

$$Y(d) = \frac{\bar{p}'(d)}{1 + d^s} + \frac{1}{1 + d} = \frac{\bar{p}'(d)}{1 + d^s} + 1 + d + d^2 + \dots + \dots$$

$$\text{i.e. } Y(d) = \frac{\bar{p}'(d)}{1 + d^s}, \quad (3.68)$$

same as obtained in Equation (3.20).

### 3.9 Critical State and Output of a Composite Sequence

Consider a sequence which is a linear combination of sequences. The critical state for each constituent sequence and the response of the scrambler in that state are known. Let us now investigate whether the response for the composite sequence can be obtained from the responses for constituent sequences.

Let  $x_1(nT), x_2(nT), \dots, x_r(nT)$  be sequences of period  $s$  ( $s \neq rq$ ) given as input to a scrambler of cycle length  $q$ .

From Equation (3.19), for each input the output transform for non-zero initial states can be written as

$$y_i(d) = \frac{p_i'(d)}{1+d^s} + \frac{q(d) A_i(d) + s_i(d)}{1+d^q} \quad (3.69)$$

If the composite signal given by

$$x(nT) = x_1(nT) + x_2(nT) + \dots + x_r(nT)$$

is given as input, then the output transform  $Y(d)$  for zero initial state is given by

$$\begin{aligned} Y(d) &= Y_1'(d) + Y_2'(d) + \dots + Y_r'(d) \\ &= \frac{1}{(1+d^s)} [p_1'(d) + p_2'(d) + \dots + p_r'(d)] \\ &\quad + \frac{q(d)}{(1+d^q)} [A_1(d) + A_2(d) + \dots + A_r(d)] \\ &= \frac{1}{(1+d^s)} \sum_{i=1}^r p_i'(d) + \frac{q(d)}{(1+d^q)} \sum_{i=1}^r A_i(d) \end{aligned}$$

For non-zero initial states we have

$$Y(d) = \frac{1}{(1+d^s)} \sum_{i=1}^r p_i'(d) + \frac{q(d)}{(1+d^q)} \left[ \sum_{i=1}^r A_i(d) + s(d) \right] \quad (3.71)$$

From Equation (3.71) it follows that  $s(d)$  will correspond to the critical state for the composite sequence  $x(nT)$  if

$$s(d) = \sum_{i=1}^r s_i(d) \quad (3.72)$$

where  $s_i(d)$  corresponds to the critical state for  $x_i(nT)$ . The output transform for each  $x_i(nT)$  alone when the scrambler is in critical state is given by

$$Y_i(d) = \frac{p_i^r(d)}{1 + d^s} \quad (3.73)$$

Also the output transform for the composite sequence  $x(nT)$ , when the scrambler is in critical state, is given by

$$Y(d) = \frac{1}{(1 + d^s)} \sum_{i=1}^r p_i^r(d) \quad (3.74)$$

From Equations (3.72), (3.73) and (3.74), we can state the following.

If the input sequence  $x(nT)$  of period  $s$  ( $\neq rq$ ) can be expressed as,

$$x(nT) = \sum_{i=1}^r a_i x_i(nT), \quad a_i \in \{0,1\} \quad (3.75)$$

then, in the critical state  $X_C$ , the output sequence is given by

$$Y(nT) = \sum_{i=1}^r a_i y_i(nT) \quad (3.76)$$

where  $y_i(nT)$  is the response for  $x_i(nT)$  when the scrambler is in critical state  $X_{C,i}$  and the critical state  $X_C$  is given by

$$X_C = \sum_{i=1}^r a_i X_{C,i} \quad (3.77)$$

**Example 3.5:** Consider the three stage scrambler with characteristic polynomial  $c(x) = x^3 + x + 1$ . The critical states and outputs for four input sequences of period 5 are listed in the Table 3.4.

Table 3.4 Critical States and Responses

Serial No. (i)	Input Sequences $x_i(nT)$	Critical States $x_{c,i}$			Output Sequences $y_i(nT)$
		$x_0$	$x_1$	$x_2$	
1	10000,10...	1	0	0	11001,11...
2	01000,01...	0	0	1	11100,11...
3	00010,00...	1	1	1	00111,00...
4	00001,00...	1	1	0	10011,10...
5	11011,11...	1	0	0	10001,10...

Note that  $x_5(nT)$  is given by

$$x_5(nT) = \sum_{i=1}^4 x_i(nT)$$

$$\therefore y_5(nT) = \sum_{i=1}^4 y_i(nT) \quad \text{and}$$

$$x_{c,5} = \sum_{i=1}^4 x_{c,i}$$

which is true as verified from the Table 3.4.

## CHAPTER 4

### SPECTRAL THEORY OF LSC AND ITS APPLICATION TO SCRAMBLERS

In this chapter first we give a brief introduction to linear sequential circuit (LSC) in general. In Section 4.2 we discuss under what conditions the response of a composite sequence over  $GF(2)$  or any of its extensions can be obtained by the sum total of responses due to constituent sequences. In Section 4.3 we discuss a method of obtaining a set of basis functions for the vector space of periodic Galois functions characterized by difference equations. This method is made use of in Section 4.4 for obtaining basis functions for the vector space of periodic Galois sequences of period equal to the cycle length of the scrambler, which when given as input to the scrambler results in an output sequence of the same period, irrespective of initial state. In Section 4.5 we give a method to obtain Fourier series expansion of periodic binary sequences over extension fields of  $GF(2)$ . In Section 4.6, we discuss concept of eigensequences and eigenvalues of LSCs. This concept is made use of in Section 4.7 to carry out spectral analysis at input and at output of 2, 3, 4 and 5 stage scramblers for various cases of input and output periods, taking eigensequences appropriately from extension fields  $GF(2^2)$ ,  $GF(2^3)$ ,  $GF(2^4)$  and  $GF(2^5)$ . Some general observations are given at the end of the section. Operation tables for various extension fields are given in Appendix A.

#### 4.1 Linear Sequential Circuits (LSC)

A block diagram of a LSC is shown in Figure 4.1.

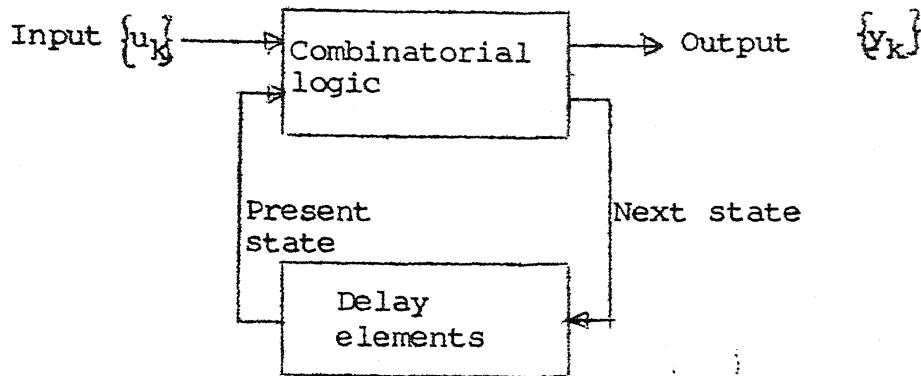


Figure 4.1 Block Diagram of a LSC.

Essentially it is made up of delay elements which serve as the memory and logic networks constructed from logic elements which perform the Galois field operations of addition and multiplication by a constant. An input sequence  $\{u_k\}$  applied to a LSC results in an output sequence  $\{y_k\}$  which is a linear function of the present input value and the present state. The present state in turn is a linear function of past states and past inputs.

A linear continuous system is characterized by a set of first-order differential equations. In the case of a LSC, it is characterized by a set of first-order difference equations. These equations can be written in matrix form as

$$x_{k+1} = Ax_k + Bu_k \quad (4.1a)$$

$$y_k = Cx_k + Du_k \quad (4.1b)$$

where,  $X$  is state vector,  $u$  and  $y$  are input and output vectors respectively. For single input single output LSC  $u$  and  $y$  are

both one-tuples. The characterizing matrices A, B, C and D are finite field valued and of consistent dimensions. The matrix A governs the autonomous behaviour of the LSC and is called characteristic matrix.

Let  $X_0$  denote the initial condition or state of the machine at  $k = 0$ . Then, it can be shown that

$$y_k = CA^k X_0 + \sum_{j=0}^{k-1} CA^{k-j-1} Bu_j + Du_k \quad (4.2)$$

We can see that the response of the system has two parts, one is zero input response and the other is zero state response. Representing these by  $\{y_{zi,k}\}$  and  $\{y_{zs,k}\}$  respectively, we can write

$$y_k = y_{zi,k} + y_{zs,k} \quad (4.3)$$

where

$$y_{zi,k} = A^k X_0 \quad (4.4)$$

$$\text{and } y_{zs,k} = \sum_{j=0}^{k-1} CA^{k-j-1} Bu_j + Du_k \quad (4.5)$$

#### 4.2 Total Response from Responses to Component Sequences

Let the input sequence  $\{u_k\}$  be expressed as a bit by bit sum of its component sequences, i.e.

$$u_k = \sum_{i=1}^r u_{i,k}$$

then let us investigate under what conditions the output sequence is given by

$$y_k = \sum_{i=1}^r y_{i,k}$$

where the sequence  $\{y_{r,k}\}$  is the output for the input sequence  $\{u_{r,k}\}$  alone. Let

$$x_{1,0} = x_{2,0} = \dots = x_{r,0} = x_0, \text{ i.e. when } k = 0.$$

Then from Equation (4.1(a)) we can write

$$x_{1,1} = Ax_0 + Bu_{1,0}$$

$$x_{1,2} = A^2x_0 + ABu_{1,0} + Bu_{1,1}$$

$$\vdots$$

$$x_{1,k} = A^kx_0 + A^{k-1}Bu_{1,0} + \dots + ABu_{1,k-2} + Bu_{1,k-1}$$

Similarly,

$$x_{2,k} = A^kx_0 + A^{k-1}Bu_{2,0} + \dots + ABu_{2,k-2} + Bu_{2,k-1}$$

$$\vdots$$

$$x_{r,k} = A^kx_0 + A^{k-1}Bu_{r,0} + \dots + ABu_{r,k-2} + Bu_{r,k-1}$$

By adding

$$\sum_{i=1}^r x_{i,k} = \underbrace{A^kx_0 + \dots + A^kx_0}_{r \text{ times}} + A^{k-1}Bu_0 + \dots + ABu_{k-2} + Bu_{k-1} \quad (4.6)$$

Also, for the input sequence  $\{u_k\}$  we can write

$$x_k = A^kx_0 + A^{k-1}Bu_0 + \dots + ABu_{k-2} + Bu_{k-1} \quad (4.7)$$

From Equation (4.6) and Equation (4.7) it follows that

$$\sum_{i=1}^r x_{i,k} = x_k \quad \text{if} \quad \begin{aligned} & (i) x_0 = 0 \text{ or} \\ & (ii) rA^kx_0 = A^kx_0 \end{aligned} \quad (4.8)$$

The second condition is satisfied for any odd number  $r$  since the operation is of characteristic 2; i.e. if the input is split into odd number of component sequences. Now for each  $\{u_{i,k}\}$ , the output can be written as,

$$y_{i,k} = CX_{i,k} + Du_{i,k}$$

$$\therefore \sum_{i=1}^r y_{i,k} = C \sum_{i=1}^r X_{i,k} + D \sum_{i=1}^r u_{i,k} = C \sum_{i=1}^r X_{i,k} + Du_k \quad (4.9)$$

Also for input sequence  $\{u_k\}$ , we have

$$y_k = CX_k + Du_k \quad (4.10)$$

From Equation (4.8) and Equation (4.10) we can say that

$$y_k = \sum_{i=1}^r y_{i,k}$$

if  $X_0 = 0$  or the input sequence is split into odd number of component sequences otherwise to the summation of individual responses, we must add the zero input response to get the total response  $y_k$ , i.e.

$$y_k = A^k X_0 + \sum_{i=1}^r y_{i,k} \quad \text{if } r \text{ is even.} \quad (4.11)$$

#### 4.3 Basis Functions for the Vector Space of Periodic Galois Functions [2]

In a continuous linear system characterised by differential equations, various signals in the system are represented by using functions such as  $e^{-at}$ ,  $e^{-at} \sin \omega t$  and  $t^2 e^{-at} \cos \omega t$ . There is a corresponding set of functions which are used to

describe the signals in linear machines. One such function is the exponent function as defined below.

Let  $\beta$  be any non-zero element of  $GF(p^n)$ . Then the function

$$e(t) = \beta^t$$

which is defined for all integral values of  $t$ , is called the exponent function. If  $\beta$  is of order  $k$ , then

$$\beta^{t+k} = \beta$$

Hence  $e(t)$  has period  $k$ . For example if  $\beta = \alpha^5$  where  $\alpha^5 \in GF(2^4)$  then

$$e(t) = (\alpha^5)^t = 1 \ \alpha^5 \ \alpha^{10} 1 \ \alpha^5 \ \alpha^{10} \dots \text{ for } t = 0, 1, \dots$$

The response of a system to an exponent function is called its exponential response.

Periodic Galois Functions: Any sequence  $g(t)$  defined for integer values of  $t$  and taking values from a Galois field  $GF(p^n)$  is called a Galois function. The linear delay operation apply to these functions. The delay operation is indicated as  $D^i g(t) = g(t-i)$  where  $D$  is referred to as the delay or  $D$  operator. If  $g(t)$  is such that  $g(t) = g(t-T)$ , then the smallest  $T$  for which this is so is called the period of  $g(t)$ .

Periodic Galois functions are not amenable to representation in a simple closed form. Instead, these functions can be defined in terms of the solution to linear difference equations. The general form of such an equation can be written as

$$g(t) + a_1 g(t-1) + \dots + a_q g(t-q) = 0 \quad (4.12)$$

where  $a_i$ 's are selected from  $GF(p^n)$ . Using the delay operator  $D$ , this equation can be written as,

$$[1 + a_1 D + \dots + a_q D^q] g(t) = F(D)g(t) = 0 \quad (4.13)$$

The polynomial  $F(D)$  is referred to as a delay polynomial, and a function  $g(t)$ , which identically satisfies the equation above for all values of  $t$ , is said to be a solution to the delay equation. For example any periodic function with period  $T_0$  will satisfy the equation  $[1 - D^{T_0}] g(t) = 0$ .

The set  $S_F$  of all such  $g(t)$  which satisfy Equation (4.13) form a  $q$  dimensional vector space over  $GF(p^n)$ . This space is invariant under linear delay operator  $D$ . Any function  $g(t)$  in this space can be written as

$$g(t) = \sum_{i=1}^q b_i \phi_i(t) \quad (4.14)$$

where  $\phi_1(t), \phi_2(t), \dots, \phi_q(t)$  form a set of  $q$  linearly independent functions; i.e. they form a basis for  $S_F$ . Now let us see how these basis functions can be obtained.

Any polynomial  $F(D)$  can be written as the product of its prime factors, i.e.

$$F(D) = [\mu_1(D)]^{e_1} [\mu_2(D)]^{e_2} \dots [\mu_r(D)]^{e_r} \quad (4.15)$$

where  $\mu_i(D)$  is an irreducible polynomial of degree  $q_i$ . Each factor  $[\mu_i(D)]^{e_i}$  corresponds to a linear subspace and associated with each, is a set of  $q_i e_i$  basis functions

$$\left\{ (k) \phi_{i,j}(t) \quad j = 1, 2, \dots, q_i, \quad k = 1, 2, \dots, e_i \right\}$$

spanning a vector space  $S_{[\mu_i(D)]^{e_i}}$ . If  $\{\phi_{i,j}^{(k)}(t)\}$  and  $\{\phi_{g,j}^{(k)}(t)\}$  are the basis functions corresponding to factors  $[\mu_i(D)]^{e_i}$  and  $[\mu_g(D)]^{e_g}$  respectively, then the basis associated with  $F(D) = [\mu_i(D)]^{e_i} [\mu_g(D)]^{e_g}$  is  $\{\phi_{i,j}^{(k)}(t)\} \cup \{\phi_{g,j}^{(u)}(t)\}$ .

Thus we can find a way to obtain basis for each subspace

$S_{[\mu_i(D)]^{e_i}}$  then 'union' of all such basis gives a basis for the vector space  $S_F$ .

To find the basis functions associated with  $[\mu_i(D)]^{e_i}$  first select  $q_i$  functions that satisfy the delay equation  $\mu_i(D) g(t) = 0$ . Next  $q_i$  functions are selected so that they satisfy

$$[\mu_i(D)]^2 g(t) = 0, \text{ but not } \mu_i(D) g(t) = 0.$$

This is done successively to obtain  $e_i^{\text{th}}$  set of  $q_i$  basis functions so that they satisfy

$$[\mu_i(D)]^{e_i} g(t) = 0 \text{ but not } [\mu_i(D)]^{e_i-1} g(t) = 0$$

Now consider  $[\mu(D)]^e = 1 + a_1 D + \dots + a_q D^q$ . Let  $T_o$  be any value of  $T$  such that  $[\mu(D)]^e$  divides  $[1 - D^{T_o}]$ . Then the period of every element in  $S$  will have a period which is a divisor of  $T_o$ . To generate the basis function of  $S$  first generate the function  $h(t)$  such that

$$h(t) = \begin{cases} 1 & t = nT_o, n = 0, 1, \dots \\ 0 & \text{otherwise} \end{cases} \quad (4.16)$$

which satisfies the equation  $[1 - D^{T_o}] h(t) = 0$ . Using  $h(t)$  the function  $\phi_1^{(1)}(t)$  can be generated as

$$(1) \phi_1(t) = \frac{(1 - D^{T_0})}{\mu(D)} h(t) \quad (4.17)$$

Note that the function is not zero and that  $\mu(D) (1) \phi_1(t) = 0$ . Hence it is selected as first basis function. If  $q = 1$  this will be the only basis function. Otherwise other  $q-1$  basis functions are given by

$$(1) \phi_i(t) = D^{i-1} [(1) \phi_1(t)] , \quad i = 2, \dots, q \quad (4.18)$$

In a similar manner the  $q$  basis functions associated with  $[\mu(D)]^j$  for  $j = 2, 3, \dots, e$  are given by

$$(j) \phi_i(t) = D^{i-1} \left[ \frac{1 - D^{T_0}}{[\mu(D)]^j} \right] h(t) , \quad i = 1, 2, \dots, q \quad (4.19)$$

After obtaining basis functions associated with each prime factor, the basis for the vector space  $S_F$  is obtained as the union of all these basis functions.

Example 4.1: Consider a function  $g(t)$  such that

$$F(D) g(t) = (1 + D^2 + D^3 + D^4) g(t) = 0$$

We can write  $F(D)$  as

$$F(D) = (1 + D)(1 + D + D^3) .$$

Basis Associated with  $1+D$ : Since  $(1 + D)$  is a divisor of  $(1 + D)$  itself

$$h(t) = 11111111\dots$$

$$\text{and } (1) \phi_1(t) = \frac{1 + D}{1 + D} h(t) = h(t)$$

$$\text{i.e. } \phi_1(t) = 11111111\dots$$

Basis Associated with  $1 + D + D^3$ : The factor  $(1 + D + D^3)$  divides  $1 + D^7$

$$\therefore h(t) = 1000000100\dots$$

$$\text{and } {}^{(1)}\phi_1(t) = \frac{1 + D^7}{1 + D + D^3} h(t) = (1 + D + D^2 + D^4) h(t)$$

$$= h(t) + h(t-1) + h(t-2) + h(t-4)$$

$$\text{i.e. } {}^{(1)}\phi_1(t) = 1110100\dots$$

$$\therefore {}^{(1)}\phi_2(t) = D \frac{1 + D^7}{1 + D + D^3} h(t)$$

$$= (D + D^2 + D^3 + D^5) h(t)$$

$${}^{(1)}\phi_2(t) = 0111010\dots$$

$$\text{and } {}^{(1)}\phi_3(t) = D^2 \frac{1 + D^7}{1 + D + D^3} h(t)$$

$$= (D^2 + D^3 + D^4 + D^6) h(t)$$

$$\therefore {}^{(1)}\phi_3(t) = 0011101\dots$$

Hence we have obtained a basis for the space  $S_F$  and the basis functions are,

$$\phi_1(t) = 1111111\dots$$

$$\phi_2(t) = 1110100\dots$$

$$\phi_3(t) = 0111010\dots$$

$$\phi_4(t) = 0011101\dots$$

#### 4.4 Application to Scramblers

Now we apply the method of the previous section to three and four stage scramblers for obtaining input sequences of periodicity equal to cycle length  $q$  and giving rise to output sequences of the same period.

Illustration 4.1: If Figure 4.2, a three stage scrambler with characteristic polynomial  $X^3 + X + 1 = 0$  with a periodic input of period 7 is represented.

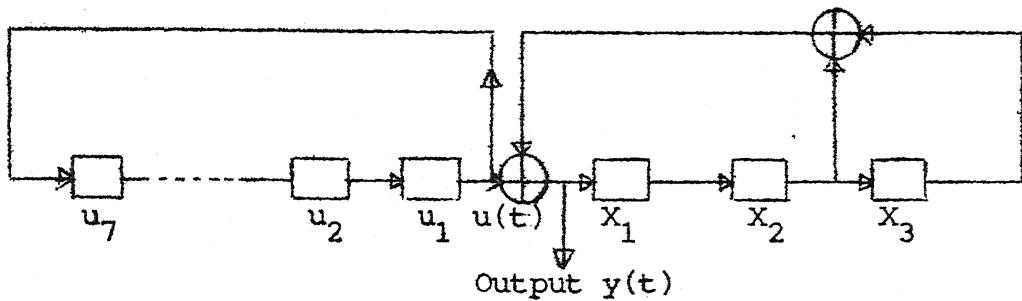


Figure 4.2 Three Stage Scrambler:  $c(x) = x^3 + x + 1$ .

If the initial state vector is  $z = [u_7 \ u_6 \ \dots \ u_1 \ x_1 \ x_2 \ x_3]^T$ , then the state vector at any instant  $k$  is given by

$$z^k = T^k z$$

where  $T$  is the transition matrix given by

T =

From this,  $T^7$  can be found to be given by

$$T^7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Since the output  $y(t)$  is given by,  $y(t) = [T^1 z]_8, [T^2 z]_8, \dots, [T^k z]_8 \dots$  where  $[z]_n$  stands for value at  $n^{\text{th}}$  location of the vector  $z$ . Hence it follows that for the output to be of period 7,

$$z^7 = T^7 z = z.$$

If this condition is to be satisfied irrespective of initial state of the scrambler, the input sequence  $u(t)$  must satisfy following equations, i.e.

$$u_7 + u_5 + u_4 + u_3 = 0$$

$$u_6 + u_4 + u_3 + u_2 = 0 \quad (4.20)$$

$$u_5 + u_3 + u_2 + u_1 = 0.$$

Writing in the delay polynomial form Equation (4.20) becomes,

$$(1 + D^2 + D^3 + D^4) u(t) = 0$$

$$D(1 + D^2 + D^3 + D^4)u(t) = 0 \quad (4.21)$$

$$D^2(1 + D^2 + D^3 + D^4)u(t) = 0$$

Any solution to above equations is an input sequence  $u(t)$  of period 7 resulting in output period of 7 itself. As discussed in Section 4.3, all such input functions  $u(t)$ , form a vector space  $S_{F(D)}$  where

$$F(D) = 1 + D^2 + D^3 + D^4 \quad (4.22)$$

We have obtained a basis for this space in Example 4.1. The basis functions are

$$\begin{aligned} \emptyset_1(t) &= 1111111\dots \\ \emptyset_2(t) &= 1110100\dots \\ \emptyset_3(t) &= 0111010\dots \\ \emptyset_4(t) &= 0011101\dots \end{aligned} \quad (4.23)$$

Note that the basis functions  $\emptyset_2(t)$ ,  $\emptyset_3(t)$  and  $\emptyset_4(t)$  spans the vector space of  $2^3$  sequences generated by the 3 stage M-sequence generator with characteristic polynomial  $c(x) = x^3 + x^2 + 1$ . Also it can be seen that (a) there are  $(2^4 - 2) = 14$  sequences excluding all zero and all one sequences of period 7 giving rise to output period of 7 itself irrespective of initial state of the scrambler, (b) these 14 sequences are M-sequences generated by the structure with characteristic polynomial  $c(x) = x^3 + x^2 + 1$  and their complements. These facts confirm observations made in Section 3.7.

Similarly for a scrambler structure of characteristic polynomial  $c(x) = x^3 + x^2 + 1$ , it can be shown that any input sequence  $u(t)$  of period 7 and giving rise to output period 7 itself irrespective of initial state, must satisfy the equation

$$F(D) u(t) = (1 + D)(1 + D^2 + D^3) y(t) = 0$$

A basis for the vector space formed by such functions can be shown to be

$$\begin{aligned}\emptyset_1(t) &= 1111111\dots \\ \emptyset_2(t) &= 1011100\dots \\ \emptyset_3(t) &= 0101110\dots \\ \emptyset_4(t) &= 0010111\dots\end{aligned}\tag{4.24}$$

Note that the basis functions  $\emptyset_2(t)$ ,  $\emptyset_3(t)$  and  $\emptyset_4(t)$  spans the vector space of  $2^3$  sequences generated by the 3 stage M-sequence generator of characteristic polynomial  $c(x) = x^3 + x + 1$ . Also it can be seen that

- (a) there are 14 sequences excluding all zero and all one sequences of period 7 giving rise to output period 7 itself, irrespective of initial state of the scrambler.
- (b) these sequences are M-sequences generated by the structure, of characteristic polynomial  $c(x) = x^3 + x + 1$  and their complements, which is in confirmity with the observation made in Section 3.7.

Illustration 4.2: Consider a 4 stage scrambler of characteristic equation  $x^4 + x + 1 = 0$  and with a periodic input of period 15 as depicted in Figure 4.3.

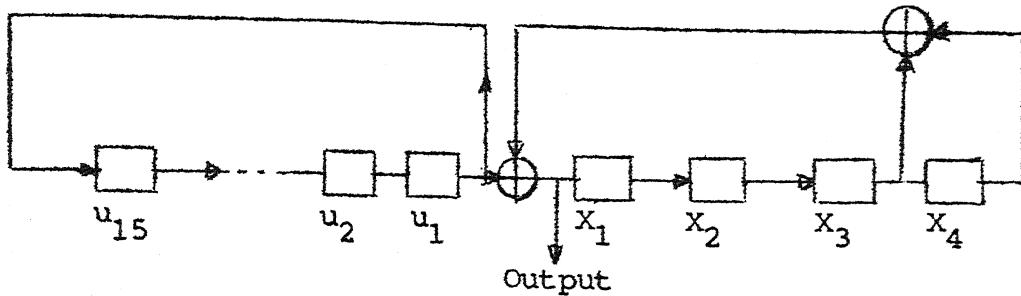


Figure 4.3 Four Stage Scrambler;  $c(x) = x^4 + x + 1$ .

Proceeding exactly like in Illustration 4.1, we can obtain following equations to be satisfied by an input sequence  $u(t)$  to give rise to output sequence of period 15 itself irrespective of initial state of the scrambler

$$\begin{aligned}
 u_{15} + u_{12} + u_{11} + u_9 + u_7 + u_6 + u_5 + u_4 &= 0 \\
 u_{14} + u_{11} + u_{10} + u_8 + u_6 + u_5 + u_4 + u_3 &= 0 \\
 u_{13} + u_{10} + u_9 + u_7 + u_5 + u_4 + u_3 + u_2 &= 0 \\
 u_{12} + u_9 + u_8 + u_6 + u_4 + u_3 + u_2 + u_1 &= 0
 \end{aligned} \tag{4.25}$$

Writing this using delay operator, we get

$$\begin{aligned}
 (1 + D^3 + D^6 + D^8 + D^9 + D^{10} + D^{11}) u(t) &= 0 \\
 D(1 + D^3 + D^6 + D^8 + D^9 + D^{10} + D^{11}) u(t) &= 0 \\
 D^2(1 + D^3 + D^6 + D^8 + D^9 + D^{10} + D^{11}) u(t) &= 0 \\
 D^3(1 + D^3 + D^6 + D^8 + D^9 + D^{10} + D^{11}) u(t) &= 0
 \end{aligned} \tag{4.26}$$

As discussed in Section 4.3, all such input sequences  $u(t)$  form a vector space  $S_F(D)$ , where

$$F(D) = 1 + D^3 + D^4 + D^6 + D^8 + D^9 + D^{10} + D^{11}$$

$$F(D) = (1 + D)(1 + D + D^2)(D^4 + D^3 + D^2 + D + 1)(D^4 + D + 1)$$

(4.27)

Now we will find basis functions associated with each factor.

Basis for  $(1 + D)$ : From Example 4.1, we have

$$\phi_1(t) = 11111111\dots$$

Basis for  $(1 + D + D^2)$ :  $(1 + D + D^2)$  divides  $(1 + D^3)$

$$\therefore h(t) = 1001001001\dots$$

$$\begin{aligned} \therefore \phi_2(t) &= \frac{1 + D^3}{1 + D + D^2} h(t) \\ &= (1 + D) h(t) = 110110110\dots \end{aligned}$$

$$\text{and } \phi_3(t) = D\phi_2(t) = 011011011\dots$$

Basis for  $(1 + D + D^4)$ :  $(1 + D + D^4)$  divides  $1 + D^{15}$ . Hence

$$h(t) = 1000000000000000,100\dots$$

$$\begin{aligned} \therefore \phi_4(t) &= \frac{1 + D^{15}}{1 + D + D^4} h(t) \\ &= 1 + D + D^2 + D^3 + D^5 + D^7 + D^8 + D^{11} h(t) \end{aligned}$$

$$\phi_4(t) = 111101011001000\dots$$

$$\phi_5(t) = D\phi_4(t) = 011110101100100\dots$$

$$\phi_6(t) = D^2\phi_4(t) = 001111010110010\dots$$

$$\phi_7(t) = D^3\phi_4(t) = 000111101011001\dots$$

Basis for  $(D^4 + D^3 + D^2 + D + 1)$ :  $(D^4 + D^3 + D^2 + D + 1)$   
divides  $1 + D^5$

$$\therefore h(t) = 10000, 100\dots$$

Basis function associated with this are,

$$\begin{aligned}\phi_8(t) &= \frac{1 + D^5}{D^4 + D^3 + D^2 + D + 1} h(t) \\ &= (1 + D) h(t)\end{aligned}$$

$$\therefore \phi_8(t) = 1100011000\dots$$

$$\phi_9(t) = D\phi_8(t) = 01100, 01100\dots$$

$$\phi_{10}(t) = D^2\phi_8(t) = 00110, 00110\dots$$

$$\phi_{11}(t) = D^3\phi_8(t) = 00011, 00011\dots$$

Hence, a set of basis functions for  $S_{F(D)}$  are,

$$\phi_1(t), \phi_2(t), \dots, \phi_{10}(t) \text{ and } \phi_{11}(t).$$

From this, it can be seen that

(a) there are  $2^{11} - 2^3 - 2 + 2^5 - 2 - 2 = 2010$  sequences  
of period 15 which gives rise to output period of 15  
irrespective of initial state.

(b) there is a subspace spanned by functions  $\phi_1(t), \phi_4(t),$   
 $\phi_5(t), \phi_6(t)$  and  $\phi_7(t)$  consisting of all sequences generated  
by the M-sequence generator with characteristic  
polynomial  $c(x) = x^4 + x^3 + 1$ , and sequences complement  
to them, which is in confirmity with the observation made  
in Section 3.7.

Similarly, for the scrambler with characteristic polynomial  $c(x) = x^4 + x^3 + 1$ , we can get a condition that is to be satisfied by an input sequence of period 15, to give rise to output period 15 irrespective of initial state. The condition is,

$$F(D) u(t) = (1 + D)(1 + D + D^2)(D^4 + D^3 + D^2 + D + 1) \\ (D^4 + D^3 + 1) u(t) = 0 \quad (4.25)$$

We have already obtained basis function associated with first three factors earlier. Hence let us obtain basis functions associated with  $(D^4 + D^3 + 1)$ .  $(D^4 + D^3 + 1)$  divides  $1 + D^{15}$ . Hence  $h(t)$  can be taken as,

$$h(t) = 1000000000000000,100\dots$$

and a set of basis functions can be obtained as

$$\emptyset_4(t) = \frac{1 + D^{15}}{D^4 + D^3 + 1} h(t) \\ = 1 + D^3 + D^4 + D^6 + D^8 + D^9 + D^{10} + D^{11} h(t)$$

$$\emptyset_4(t) = 100110101111000\dots$$

$$\emptyset_5(t) = D\emptyset_4(t) = 010011010111100\dots$$

$$\emptyset_6(t) = D^2\emptyset_4(t) = 001001101011110\dots$$

$$\emptyset_7(t) = D^3\emptyset_4(t) = 000100110101111\dots$$

These four functions and functions  $\emptyset_1(t)$ ,  $\emptyset_2(t)$ ,  $\emptyset_3(t)$ ,  $\emptyset_8(t)$ ,  $\emptyset_9(t)$ ,  $\emptyset_{10}(t)$  and  $\emptyset_{11}(t)$  obtained earlier constitute a basis for the vector space of all such functions  $u(t)$  satisfying Equation (4.28). From this it can be seen that

(a) there are  $2^{11} - [2^3 - 2 + 2^5 - 2] - 2 = 2010$  sequences of periodicity 15 resulting in output period 15 itself irrespective of initial state,

(b) there is a subspace spanned by basis functions  $\emptyset_1(t)$ ,  $\emptyset_4(t)$ ,  $\emptyset_5(t)$ ,  $\emptyset_6(t)$  and  $\emptyset_7(t)$  consisting of all sequences generated by the M-sequence generator with characteristic polynomial  $c(x) = x^4 + x + 1$ , and sequences complement to them, which is in confirmity with the observations made in Section 3.7.

#### 4.5 Fourier Series Expansion of Periodic Binary Sequences Over Finite Fields

A periodic real or complex signal can be expressed as an infinite sum of exponential functions in complex field. Similarly in the case of a periodic function over  $GF(p)$  it is possible to express this as a finite sum of exponent function over an appropriate extension field  $GF(p^n)$ . The difficulty in this case is that it is possible to do so for periodic signals with certain periodicities only. Only such functions having a periodicity  $i$ , where  $i$  is a divisor of  $p^i - 1$  can be expressed in this form. For sequences over  $GF(2)$  satisfying above constraint, we give below a method for obtaining Fourier series expansion.

From Equation (2.5) it is clear that  $(x^{p^m-1} - 1)$  splits into  $(p^m - 1)$  linear factors in  $GF(p^m)$ , i.e.

$$(x^{p^m-1} - 1) = (x - \alpha^0)(x - \alpha) \dots (x - \alpha^{p^m-2})$$

Hence all non-zero field elements are various roots of unity.

Now consider a matrix  $M$  whose columns consist of exponent

functions of non-zero elements  $\alpha^0$  to  $\alpha^{p^m-2}$ . The matrix M has following properties.

- (a) It is a square matrix of dimension  $(p^m-1) \times (p^m-1)$
- (b) M is a symmetric matrix since

$$m_{ij} = (\alpha^j)^i = (\alpha^i)^j = m_{ji}, \quad i = 0, \dots, p^m-2$$

$$j = 0, \dots, p^m-2$$

(4.29)

- (c) For each column j, there is a column k such that

$m_{ik} = m_{ij}^{-1}$  because, for every element  $\alpha^j$  there is an inverse  $\alpha^k$  and if that is so

$$(\alpha^k)^i = [(\alpha^j)^{-1}]^i = [(\alpha^j)^i]^{-1}$$

$$\text{i.e. } m_{ik} = m_{ij}^{-1} \quad (4.30)$$

(Note that the first column is all ones and hence it is its own inverse). Also for such columns j and k

$$\sum_{i=0}^{p^m-2} (m_{ik})(m_{ij}) = \sum_{i=0}^{p^m-2} (m_{ik})(m_{ik}^{-1}) = p^m-1 \mid \text{mod } p,$$

$$(\text{= 1 in } GF(2^m)) \quad (4.31)$$

- (d) Multiplication of respective elements of any two columns give another column, i.e.

$$(m_{ij})(m_{ik}) = (\alpha^j)^i (\alpha^k)^i = (\alpha^{j+k})^i = (\alpha^1)^i = m_{il}$$

$$(4.32)$$

and for any two columns j and k not satisfying the relation in (c)

$$\sum_{i=0}^{p^m-2} (m_{ik})(m_{ij}) = \sum_{i=0}^{p^m-2} m_{il} = \sum_{i=0}^{p^m-2} (\alpha^l)^i = 0 \quad (4.33)$$

From the above properties, it follows that the matrix  $M^{-1}$  can be obtained by interchanging appropriate columns of  $M$ .

Illustration 4.3: The matrix  $M$  given below is a matrix having exponent function in  $GF(2^3)$  as its columns.

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{bmatrix}$$

It can be seen that the pairs of columns  $(2, 7)$ ,  $(3, 6)$ ,  $(4, 5)$  satisfy property (c). Hence  $M^{-1}$  can be written as,

$$M^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix}$$

Now let us say a periodic binary sequence of period  $i$  (such that  $i$  is a divisor of  $2^m-1$ ) can be expressed as

$$\{a\} = a_0 a_1 \dots a_{\frac{m}{2}-2} \dots = \sum_{i=0}^{2^m-2} c_i \{\alpha^i\} \quad (4.34)$$

where  $\{\alpha^i\}$  denotes exponent function of element  $\alpha^i$ . This can be written in matrix form as

$$M \underline{C} = \underline{A} \quad (4.35)$$

$$\text{where } \underline{A} = [a_0, a_1, \dots, a_{\frac{m}{2}-2}]^T, \underline{C} = [c_0, c_1, \dots, c_{\frac{m}{2}-2}]^T$$

and the coefficients  $c_0, \dots, c_{\frac{m}{2}-2}$  can be obtained as

$$\underline{C} = M^{-1} \underline{A} \quad (4.36)$$

Once we are able to find the Fourier coefficients, the next question which arises is that whether there can be any well defined exponential response for a given LSC due to each one of these exponent functions. Because, in that case the response due to any binary sequence (with appropriate periodicity) can be obtained from exponential responses due to its constituent exponent functions. This aspect is discussed in the next section.

Example 4.2: Let us now find out the Fourier coefficients (spectrum) of the periodic sequence  $\{u_k\} = 1001011, 1001011\dots$

Let the coefficient of any  $\{e^k\}$  be denoted by  $U_e$ , where  $e \in GF(2^3)$ . Then these coefficients are obtained as

$$\underline{U}_e = M^{-1} \underline{u}_k$$

$$\text{where, } \underline{U}_e = [u_1 \ u_\alpha \ u_{\alpha^2} \ \dots \ u_{\alpha^6}]^T$$

$$\text{and } \underline{u}_k = [u_0 \ u_1 \ \dots \ u_6]^T$$

i.e.  $\underline{v}_e =$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha \\ 1 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

or  $U_1 = 1 + 1 + 1 + 1 = 0$

$$U_\alpha = 1 + \alpha^4 + \alpha^2 + \alpha = 1$$

$$U_{\alpha^2} = 1 + \alpha + \alpha^4 + \alpha^2 = 1$$

$$U_{\alpha^3} = 1 + \alpha^5 + \alpha^6 + \alpha^3 = 0$$

$$U_{\alpha^4} = 1 + \alpha^2 + \alpha + \alpha^4 = 1$$

$$U_{\alpha^5} = 1 + \alpha^6 + \alpha^3 + \alpha^5 = 0$$

$$U_{\alpha^6} = 1 + \alpha^3 + \alpha^5 + \alpha^6 = 0$$

#### 4.6 Eigensignals and Eigenvalues of LSC

We will now study 'Spectral theory' on finite fields for LSCs as suggested by Sangani [13].

For an operator  $M$  on a vector space, if there exist a scalar  $\lambda$  and a non-zero vector  $U$  such that

$$MU = \lambda U \quad (4.37)$$

then  $\lambda$  is said to be an eigenvalue and  $U$ , the corresponding eigenvector. This equality which is very familiar with real or complex matrices on a finite dimensional space also holds for an arbitrary operator on an abstract vector space. This

fact is made use of to define the eigenvalues and eigenvectors or eigenfunctions of a single input-single output LSC by viewing it as a linear operator on the infinite dimensional vector space of 'two-sided' sequences with values in  $GF(p)$ .

Hence Equation (4.1) can be written as

$$\begin{aligned} X_{k+1} &= AX_k + Bu_k \\ \lambda u_k &= CX_k + Du_k, \quad -\infty < k < \infty \end{aligned} \quad (4.38)$$

where  $\{u_k\}$  is an eigenfunction and  $\lambda$  the eigenvalue, both taking their values in some extension field of  $GF(p)$ . Any extension field of a field plays essentially the same role for an LSC defined over that field as complex numbers do for an analog circuit defined over the real field.

Consider a periodic exponent function  $\{e^k\}$ ,  $k = 0, \pm 1, \pm 2, \dots$ , as input to an LSC. Where  $e$  is an element in some extension field of  $GF(p)$  over which LSC is defined. Transfer function  $S(e)$  of this LSC is defined as

$$S(e) \triangleq D + C(eI - A)^{-1} B \quad (4.39)$$

Here  $S(e)$  is a rational function in  $e$  with coefficients in a finite field, whose poles and zeros are well defined elements of the extension field. For each  $e$ , except for the cases where  $(eI - A)^{-1}$  is not defined (does not exist), the sequence  $\{u_k\} = \{e^k\}$ ,  $-\infty < k < \infty$ , is an eigenfunction of the LSC with eigenvalue  $S(e)$ . The eigenvalues of LSC are elements of the extension field and the eigenfunctions take their values in the same extension field, just as the eigenvalues and eigenfunctions defined over the real field are complex.

The following theorem gives the condition under which  $S(e)$ , the transfer function defined earlier and the function  $\{e^k\}$  are respectively an eigenvalue and corresponding eigensequence of the LSC defined by Equation (4.38).

Theorem: Let

$$x_{k+1} = Ax_k + Bu_k \quad (4.40)$$

$$y_k = Cx_k + Du_k, \quad -\infty < k < \infty \quad (4.41)$$

characterize a LSC over a finite field. Then for each  $e$  in an extension field for which

$$S(e) \triangleq C(Ie - A)^{-1} B + D$$

is defined, there exists a unique state  $x_0 = x(e)$  such that the sequence

$$\{u_k\} = \{e^k\}, \quad k = 0, \pm 1, \pm 2, \dots$$

is an eigensequence for the LSC defined by Equation (4.40) and Equation (4.41). The corresponding eigenvalue is  $S(e)$ . The unique state  $x_0$  is given by

$$x_0 = x(e) = (Ie - A)^{-1} B. \quad (4.42)$$

It can be shown that

$$x_k = (Ie - A)^{-1} B e^k \quad (4.43)$$

is the unique solution to Equation (4.40) with  $x_0$  given by Equation (4.42). Substituting Equation (4.43) in Equation (4.41), we get

$$\begin{aligned}
 y_k &= CX_k + Du_k \\
 &= [C(Ie - A)^{-1} B + D] e^k \\
 \text{i.e. } y_k &= [S(e)] e^k
 \end{aligned} \tag{4.44}$$

Let us now consider an input sequence  $\{u_k\}$  which is a shifted version of an eigensequence  $\{e^k\}$ ; i.e.

$$\{u_k\} = b\{e^k\}, \quad b \in GF(2^n), \quad b \neq 0 \tag{4.45}$$

Then from Equation (4.43),

$$x_k = b(Ie - A)^{-1} B e^k \tag{4.46}$$

Substituting this in Equation (4.41),

$$\begin{aligned}
 y_k &= b [C(Ie - A)^{-1} B + D] e^k \\
 &= S(e) b e^k = S(e) u_k
 \end{aligned} \tag{4.47}$$

i.e., the coefficient of  $\{e^k\}$  at the output is eigenvalue times the coefficient at input. We can observe that the function  $\{u_k\}$  is an eigensequence with  $S(e)$  as eigenvalue and the unique state is given by

$$x(e, b) = b(Ie - A)^{-1} B = bX(e) \tag{4.48}$$

where  $X(e)$  is the unique state  $X_0$  such that the sequence  $e^k$  and  $S(e)$  are respectively an eigensequence and corresponding eigenvalue of the LSC.

Now consider a sequence  $\{u_k\}$  given by Equation (4.45), given as input to a LSC operating in  $GF(2)$  and whose initial

state is zero. The total response  $\{y_k\}$  can be written as

$$y_k = \sum_{j=0}^{k-1} C A^{k-j-1} B u_j + D u_k + A^k X(e, b) + A^k X(e, b)$$

From Equation (4.47) this can be written as

$$y_k = S(e) u_k + A^k X(e, b) \quad (4.49)$$

If initial state is non-zero, say  $x_a$ , then

$$y_k = S(e) u_k + A^k X(e, b) + A^k x_a \quad (4.50)$$

where first two terms give zero state response and the third term gives zero input response.

#### 4.7 Application of Spectral Theory to Scramblers

In this section we will apply spectral theory to 2, 3, 4 and 5 stage scramblers. Eigensequences  $\{e^k\}$  are taken from extension fields  $GF(2^2)$ ,  $GF(2^3)$ ,  $GF(2^4)$  and  $GF(2^5)$  in each case. Spectral analysis at input and at output of the scrambler for some class of periodic input sequences is carried out and observations made thereof are summarised at the end of the section. Throughout this section the coefficient of an eigensequence  $\{e^k\}$  at input and output are denoted by  $u_e$  and  $y_e$  respectively.

##### 4.7.1 Two Stage Scrambler:

The two stage scrambler with characteristic polynomial  $c(x) = x^2 + x + 1$  is shown in Figure 4.4.

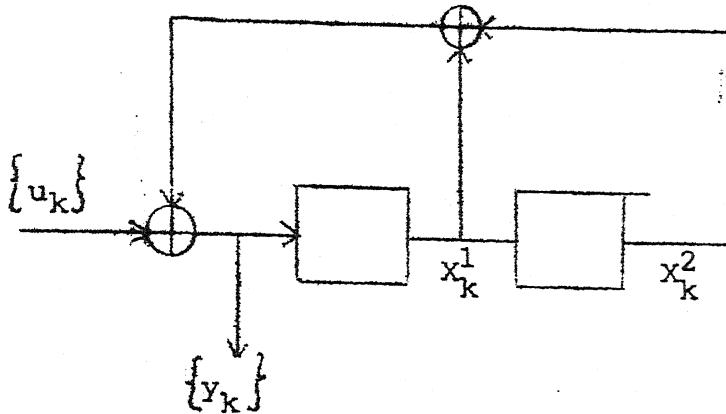


Figure 4.4 Two Stage Scrambler;  $c(x) = x^2 + x + 1$ .

The characterising equations can be written as

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k \\ y_k &= Cx_k + Du_k \end{aligned} \quad (4.51)$$

where

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad C = [1 \quad 1] \quad \text{and} \quad D = 1$$

Let us now consider eigensequences from  $GF(2^2)$ ,  $GF(2^3)$ ,  $GF(2^4)$  and  $GF(2^5)$  and we will find out spectral coefficients corresponding to each of them at the input and at the output.

(a) Eigensequences from  $GF(2^2)$ : For  $e = 1$ , the  $\text{Det}(Ie - A)$  is given by

$$\text{Det}(Ie - A) = \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} = 1$$

Therefore for  $e = 1$  eigenvalue is defined and the unique state  $x_0 = x(1)$  is given by

$$x(1) = (Ie - A)^{-1} B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\therefore s(1) = C(Ie - A)^{-1} B + D = 1 + 1 + 1 = 1$$

For  $e = \alpha$ ,

$$\text{Det}(Ie - A) = \begin{vmatrix} 1+\alpha & 1 \\ 1 & \alpha \end{vmatrix} = 0.$$

Therefore eigenvalue is not defined and  $\{\alpha^k\}$  is not an eigensequence of this LSC.

For  $e = \alpha^2$ ,

$$\text{Det}(Ie - A) = \begin{vmatrix} 1+\alpha^2 & 1 \\ 1 & \alpha \end{vmatrix} = 0.$$

Therefore eigenvalue is not defined and  $\{\alpha^{2k}\}$  is not an eigensequence of this LSC.

Now if the sequence 111... is given as input with the state  $X(1)$  then, output sequence is also 111... i.e. the Equation (4.44) is satisfied. For two stage scrambler there is only one case wherein the output is of period 3 irrespective of initial state.\* Spectral coefficients at input and at output for this case and different initial conditions are obtained as explained in Section 4.5 and are listed in Table 4.1. Spectral coefficients for zero input responses are also given in the table.

Note that:

- (i) the spectral coefficients of eigensequences  $\{\alpha^k\}$  and  $\{\alpha^{2k}\}$  for which eigenvalue is not defined, are zero at the input.
- (ii) For  $e = 1$  where eigenvalue is defined,

$$Y_1 = S(1) U_1$$

---

\* State at instant  $k = 0$ .

Table 4.1 Spectral Coefficients at Input and Output for Sequences of Period 3; 2-stage Scrambler

Initial States		Input/Output Sequences	Input/Output Spectral Coefficients		
$x_1$	$x_2$		$u_1(y_1)$	$u_\alpha(y_\alpha)$	$u_{\alpha^2}(y_{\alpha^2})$
0	0	111,...	1	0	0
		100,...	1	1	1
-----					
0	1	111,...	1	0	0
		010,...	1	$\alpha^2$	$\alpha$
-----					
1	0	111,...	1	0	0
		001,...	1	$\alpha$	$\alpha^2$
-----					
1	1	111,...	1	0	0
		111,...	1	0	0
-----					
0	1	-	-	-	-
		110,...	0	$\alpha$	$\alpha^2$
-----					
1	0	-	-	-	-
		101,...	0	$\alpha^2$	$\alpha$
-----					
1	1	-	-	-	-
		011,...	0	1	1

(iii) The new coefficients which appear in those places where eigenvalues are not defined, are due to the sequence generated by the state given by

$$X_T = U_1 X(1) + X_a \quad (4.52)$$

where  $X_a$  is actual initial state of the scrambler. This is justified by Equation (4.50).

Example 4.3: In the case when the input is 111... and initial state is 01,  $X_T$  is given by

$$X_T = \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and the sequence generated by this is 101,101.... The spectral coefficients of this are  $y_1 = 0$ ,  $y_\alpha = \alpha^2$  and  $y_{\alpha^2} = \alpha$ . From the Table 4.1 it can be seen that these are the new coefficients which appear at the output.

(b) Eigensequences from  $GF(2^3)$ : For the 2-stage scrambler, eigenvalues  $S(e)$ , for each eigenfunction  $\{e^k\}$  and their unique states  $X(e)$  are given in Table 4.2. In this case eigenvalues are defined for all eigensequences.

Now let us consider 7 basis functions which span the vector space of all 7-tuples as input. Each one of them gives rise to an output sequence of period 7 when the scramble is in critical state. The spectral coefficients at input and output for such cases are listed in Table 4.3. It can be seen that

(i) For any eigensequence  $\{e^k\}$ , its coefficient  $y_e$  at output is given by

Table 4.2 Eigenvalues and Unique States in  $GF(2^3)$ ; 2-stage Scrambler

e	x(e)		s(e)
	$x_1$	$x_2$	
1	1	1	1
$\alpha$	$\alpha^3$	$\alpha^2$	$\alpha^4$
$\alpha^2$	$\alpha^6$	$\alpha^4$	$\alpha$
$\alpha^3$	$\alpha^5$	$\alpha^2$	$\alpha$
$\alpha^4$	$\alpha^5$	$\alpha$	$\alpha^2$
$\alpha^5$	$\alpha^6$	$\alpha$	$\alpha^4$
$\alpha^6$	$\alpha^3$	$\alpha^4$	$\alpha^2$

$$y_e = s(e) u_e$$

(ii) For any input sequence,

$$\sum_e u_e x(e) = x_c \quad (4.53)$$

where  $x_c$  is the critical state for that sequence.

This can be justified as follows. From Equation (4.11) and Equation (4.50) the output response is given by

$$y_k = \sum_e u_e s(e) e^k + A^k \sum_e u_e x(e) + A^k x_c \quad (4.54)$$

In this, the response due to second and third terms is of period 3. Hence for the output period to be 7, this response should be all zeros. This will be so only if condition (ii) is satisfied.

Table 4.3 Spectral Coefficients at Input and Output for Sequences of Period 7; 2-stage Scrambler

Critical States $X_C$		Input/Output Sequences	Input/Output Spectral Coefficients						
$X_1$	$X_2$		1	$\alpha$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$
1	1	1000000,...	1	1	1	1	1	1	1
		1011011,...	1	$\alpha^4$	$\alpha$	$\alpha$	$\alpha^2$	$\alpha^4$	$\alpha^2$
<hr/>									
1	0	0100000,...	1	$\alpha^3$	$\alpha^6$	$\alpha^5$	$\alpha^5$	$\alpha^6$	$\alpha^3$
<hr/>									
0	1	0010000,...	1	$\alpha^2$	$\alpha^4$	$\alpha^2$	$\alpha$	$\alpha$	$\alpha^4$
<hr/>									
1	1	0001000,...	1	$\alpha$	$\alpha^2$	$\alpha^6$	$\alpha^4$	$\alpha^3$	$\alpha^5$
<hr/>									
1	0	0000100,...	1	1	1	$\alpha^3$	1	$\alpha^5$	$\alpha^6$
<hr/>									
0	1	0000010,...	1	$\alpha^6$	$\alpha^5$	1	$\alpha^3$	1	1
<hr/>									
1	0	0000001,...	1	$\alpha^5$	$\alpha^3$	$\alpha^4$	$\alpha^6$	$\alpha^2$	

From Section 3.9 it follows that any input sequence of period 7, when the scrambler is in critical state, will give rise to an output sequence which is some linear combination of the 7 output sequences given in Table 4.3. The corresponding critical state is given by the same linear combination of critical states listed against each output sequence. Therefore the above two properties hold good in all cases where input and output periods are 7.

Example 4.3: From Table 4.3, for the sequence 0100000,01..., we have

$$\begin{aligned}
 \sum_e u_e x_e &= \begin{bmatrix} 1 \\ 1 \end{bmatrix} + \alpha^6 \begin{bmatrix} \alpha^3 \\ \alpha^2 \end{bmatrix} + \alpha^5 \begin{bmatrix} \alpha^6 \\ \alpha^4 \end{bmatrix} + \alpha^4 \begin{bmatrix} \alpha^5 \\ \alpha^2 \end{bmatrix} \\
 &\quad + \alpha^3 \begin{bmatrix} \alpha^5 \\ \alpha \end{bmatrix} + \alpha^2 \begin{bmatrix} \alpha^6 \\ \alpha \end{bmatrix} + \alpha \begin{bmatrix} \alpha^3 \\ \alpha^4 \end{bmatrix} \\
 &= \begin{bmatrix} 1 \\ 1 + \alpha + \alpha^3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = x_c
 \end{aligned}$$

the critical state for that sequence.

(c) Eigensequences from  $GF(2^4)$ : In this case except for  $e = \alpha^5$  and  $\alpha^{10}$  for all other eigensequences, eigenvalues are defined. Eigenvalues for all eigensequences and their unique states are listed in Table 4.4. We will do the analysis for the following cases.

- (i) Input period is 5 and output period is also 5
- (ii) Input period is 5 and output period is 15
- (iii) Input period is 15 and output period is 15.

Table 4.4 Eigenvalues and Unique States in  $GF(2^4)$ ; 2-stage Scrambler

e	x(e)		s(e)
	$x_1$	$x_2$	
1	1	1	1
$\alpha$	$\alpha^6$	$\alpha^5$	$\alpha^7$
$\alpha^2$	$\alpha^{12}$	$\alpha^{10}$	$\alpha^{14}$
$\alpha^3$	$\alpha^{10}$	$\alpha^7$	$\alpha^{13}$
$\alpha^4$	$\alpha^9$	$\alpha^5$	$\alpha^{13}$
$\alpha^6$	$\alpha^5$	$\alpha^{14}$	$\alpha^{11}$
$\alpha^7$	$\alpha^3$	$\alpha^{11}$	$\alpha^{10}$
$\alpha^8$	$\alpha^3$	$\alpha^{10}$	$\alpha^{11}$
$\alpha^9$	$\alpha^5$	$\alpha^{11}$	$\alpha^{14}$
$\alpha^{11}$	$\alpha^9$	$\alpha^{13}$	$\alpha^5$
$\alpha^{12}$	$\alpha^{10}$	$\alpha^{13}$	$\alpha^7$
$\alpha^{13}$	$\alpha^{12}$	$\alpha^{14}$	$\alpha^{10}$
$\alpha^{14}$	$\alpha^6$	$\alpha^7$	$\alpha^5$

In Table 4.5 we have listed spectral coefficients at input and at output for 5 basis functions of period 5 and giving rise to output functions of period 5 itself. Obviously, only coefficients corresponding to eigensequences  $\{e^k\}$  for  $e = 1, \alpha^3, \alpha^6, \alpha^9$  and  $\alpha^{12}$  appear at the input and at output, since they are the sequences of period 5. In each case it is seen that

$$(i) \quad y_e = s(e) u_e \quad \text{for all } e$$

Table 4.5 Spectral Coefficients for Input and Output for Sequences of Period 5; 2-Stage Scrambler

Critical States $X_C$		Input/ Output Sequences	Input/Output Spectral Coefficients*											
$X_1$	$X_2$		1	0	0	1	0	1	0	0	1	0	1	0
1	0	10000, ...	1	0	0	1	0	1	0	0	1	0	1	0
		01101, ...	1	0	0	14	0	12	0	0	15	0	8	0
-----														
0	1	01000, ...	1	0	0	13	0	10	0	0	7	0	4	0
		10110, ...	1	0	0	11	0	6	0	0	6	0	11	0
-----														
1	1	00100, ...	1	0	0	10	0	4	0	0	13	0	7	0
		01011, ...	1	0	0	8	0	15	0	0	12	0	14	0
-----														
1	0	00010, ...	1	0	0	7	0	13	0	0	4	0	10	0
		10101, ...	1	0	0	5	0	9	0	0	3	0	2	0
-----														
0	1	00001, ...	1	0	0	4	0	7	0	0	10	0	13	0
		11010, ...	1	0	0	2	0	3	0	0	9	0	5	0

\*Mapping of elements:  $0 \rightarrow 0, i+1 \rightarrow \alpha^i, i = 0, 1, \dots, 14$

$$(ii) \sum_e u_e x(e) + x_c = 0$$

where  $x_c$  is the critical state for the sequence and  $e = 1, \alpha^3, \alpha^6, \alpha^9$ , and  $\alpha^{12}$ . This has to be so, otherwise output period will be  $\text{LCM}(15, 3) = 15$ .

From Section 3.9 it follows that the above conditions are satisfied in general for any sequence of period five giving rise to output sequence of period five.

Now let us consider the case when the input period of 15 resulting in output period of 15, irrespective of initial state. The cases of input period 5/3 resulting in output period 15 is also covered in this. Spectral coefficients at the input and at output for 13 basis function. When the initial state of the scrambler is zero is given in Table 4.6. The sequence 111000000000000, 111... and its shifted versions are taken as basis functions because,

Let the input transform be  $\frac{p(d)}{1 + d^{15}}$

For the two stage scrambler from Section 3.5, the transfer function is given by

$$H(d) = \frac{1}{d^2 + d + 1}$$

Therefore the output transform is given by

$$Y(d) = \frac{p(d)}{1 + d^{15}} \cdot \frac{1}{(1 + d + d^2)}, \quad \deg p(d) \leq 14.$$

In the denominator of  $Y(d)$  there are two factors of  $(1 + d + d^2)$ . Hence the exponent of the denominator can be 15 only if  $p(d)$

has a factor  $(1 + d + d^2)$ . In that case only the output period will be 15 irrespective of initial state. Otherwise the output period will be 30. Hence  $p(d)$  can be anything of the kind given by

$$p(d) = (1 + d + d^2)(a_0 + a_1 d^1 + a_2 d^2 + \dots + a_k d^k), \quad k \leq 12$$

Hence it follows that any function resulting in an output period of 15 should be some linear combination of these 13 sequences given in the table. Last three rows gives the zero input response for different states and their spectral contents.

It can be seen that

(i)  $y_e = s(e) u_e$ ,  $e \in (e)$  eigenvalue is defined for  $\{e^k\}$

(ii) The new coefficients are due to the zero input response of the state  $x_T$  given by

$$x_T = \sum_e u_e x(e) \quad \text{for all } e.$$

(iii) The spectral coefficients at the input corresponding to those places where eigenvalue is not defined are zero.

In general any output sequence is some linear combination of these 13 output sequences, plus any one of the last three output sequences for non-zero initial state. Hence it follows that for any such sequence the conditions (i), (ii) and (iii) are satisfied and the state  $x_T$  for any non-zero initial state  $x_a$  is given by

$$x_T = \sum_e u_e x_e + x_a$$

which is justified from Equation (4.50).

Table 4.6 Spectral Coefficients at Input and Output for Sequences of Period 15;  
2-stage Scrambler

Critical States $X_C$		Input/Output Sequences										Input/Output spectral Coefficients*									
00	11100000000000,...	1	9	2	3	0	5	6	5	2	0	11	9	6	11	1	1	1	1	1	1
00	10000000000000,...	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
00	01110000000000,...	1	8	15	15	14	0	14	14	12	8	0	15	12	8	12	12	12	12	12	12
00	01000000000000,...	1	15	14	13	12	11	10	9	8	7	6	5	4	3	2	2	2	2	2	2
00	00111000000000,...	1	7	13	12	10	0	8	7	4	14	0	4	15	10	13	13	13	13	13	13
00	00100000000000,...	1	14	12	10	8	6	4	2	15	13	11	9	7	5	3	3	3	3	3	3
00	00011100000000,...	1	6	11	9	6	0	2	15	11	5	0	8	3	12	14	14	14	14	14	14
00	00010000000000,...	1	13	10	7	4	1	13	10	7	4	1	13	10	7	4	4	4	4	4	4
00	00001110000000,...	1	5	9	6	2	0	11	8	3	11	0	12	6	2	13	9	15	15	15	15
00	00001000000000,...	1	12	8	4	15	11	7	3	14	10	6	1	11	6	1	1	1	1	1	1
00	0000011110000000,...	1	4	7	3	13	0	5	1	10	2	0	1	9	1	1	1	1	1	1	1
00	0000010000000000,...	1	11	6	1	11	6	1	11	6	1	11	6	1	10	4	3	2	2	2	2
00	0000001111000000,...	1	3	5	15	9	0	14	9	2	8	0	5	12	3	2	2	2	2	2	2
00	0000001000000000,...	1	10	4	13	7	1	10	4	13	7	1	10	4	3	2	2	2	2	2	2
00	0000001110000000,...	1	2	3	12	5	0	8	2	9	14	0	9	15	5	3	3	3	3	3	3
00	0000001000000000,...	1	9	2	10	3	11	4	12	5	13	6	14	7	15	8	8	8	8	8	8
00	0000000111000000,...	1	1	1	9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
00	0000000100000000,...	1	8	15	7	14	6	13	5	12	4	11	3	10	2	2	2	2	2	2	2

continued. . .

Table 4.6 (continued)

Critical States $x_C$	Input/Output Sequences		Input/Output Spectral Coefficients *														
	000000000111000, ...	000000000100000, ...	1	15	14	6	12	0	11	3	8	11	0	2	6	9	5
00	1	7	13	4	10	1	7	13	4	10	1	7	13	4	10	5	
00	000000000111000, ...	000000000100000, ...	1	14	12	3	8	0	5	11	15	2	0	6	9	11	6
00	00000000001110, ...	00000000001000, ...	1	6	11	1	6	11	1	6	11	1	6	11	1	6	11
00	000000000001110, ...	000000000001000, ...	1	13	10	15	4	0	14	4	7	8	0	10	12	13	7
00	000000000000111, ...	000000000000100, ...	1	12	8	12	15	0	8	12	14	14	0	14	15	15	8
01	110, ...	-	0	0	0	0	0	6	0	0	7	10	13	1	4	7	10
10	101, ...	-	0	0	0	0	0	11	0	0	0	0	6	0	0	0	0
11	011, ...	-	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0

\*Table should be read with following mapping for input/output spectral coefficients column

$0 \rightarrow 0$  and

$1 + 1 \rightarrow \alpha^1, \quad 1 = 0, 1, \dots, 14.$

(d) Eigensequences from  $GF(2^5)$ : In this extension field, we will consider cases having input and output periods 31. Table 4.7 gives the eigenvalues and unique state for each eigensequences. Spectral coefficients for 31 basis functions at input and at output along with their critical states are given in Table 4.8. It can be seen that

$$(i) \quad y_e = u_e s(e) , \quad \text{for all } e.$$

$$(ii) \quad \sum_e u_e x(e) = x_c$$

in each case. Hence from Section 3.9 it follows that in all cases of input period of 31 resulting in an output period of 31, the conditions (i) and (ii) are satisfied.

#### 4.7.2 Three Stage Scrambler:

We will analyse the three stage scrambler structure shown in Fig. 4.5. for the following cases

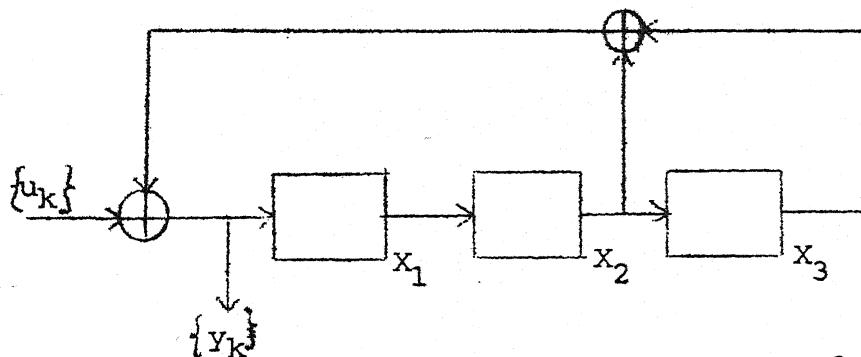


Figure 4.5 Three-stage Scrambler;  $c(x) = x^3 + x + 1$ .

- (i) Input and output periods 3
- (ii) Input and output period 7
- (iii) Input and output period 5

Table 4.7 Eigenvalues and Unique States in  $GF(2^5)$ :  
2-Stage Scrambler.

e	X(e)		S(e)
	X <sub>1</sub>	X <sub>2</sub>	
1	1	1	1
2	22	21	23
3	12	10	14
4	17	14	20
5	23	19	27
6	15	10	20
7	2	27	8
8	5	29	12
9	14	6	22
10	20	11	29
11	29	19	6
12	26	15	6
13	3	22	15
14	8	26	21
15	9	26	23
16	27	12	11
17	27	11	12
18	9	23	26
19	8	21	26
20	3	15	22
21	26	6	15
22	29	8	19
23	29	29	11
24	14	22	6
25	5	12	29
26	2	4	27
27	15	20	10
28	23	27	19
29	17	20	14
30	12	14	10
31	22	23	21

\* Mapping of elements: 0---->0; i+1---->a<sup>i</sup>, i=0,1,2,...,31.

Table 4.8 Spectral Coefficients at Input and Output for Sequences of Period 3 ( $c(x) = x + 1$ )

(cont'd.)

Table 4.6 contd

$s_1$	$s_0$	Initial State	Input/Output spectral Coefficients
22	0	1	1 11 21 31 10 20 30 9 19 29 8 18 28 7 17 27 6 16 26 5 15 25 4 14 24 3 13 22 2 12 26 1 2 3 19 5 8 6 20 9 26 15 23 11 27 8 6 17 10 20 25 20 12 14 19 21 29 22 10 15 21 31
23	1	0	0 10 19 28 9 15 24 2 11 20 29 7 16 25 3 12 21 30 8 17 26 7 13 22 31 9 18 27 6 14 23 1 1 1 16 1 3 31 13 1 17 5 12 3 11 25 22 1 24 2 2 7 6 29 25 27 28 4 21 14 1 23 12
24	0	1	1 9 17 25 2 10 18 26 3 11 19 27 4 12 20 29 5 13 24 29 2 13 22 30 7 15 23 31 3 16 24 1 31 30 13 28 29 25 6 24 3 20 11 13 1 11 7 16 7 15 1 23 1 1 4 4 17 1 18 21 25 13
25	1	1	8 15 22 29 5 12 19 26 2 16 23 30 9 13 20 27 3 10 17 21 31 7 13 21 28 4 11 18 25 1 39 28 10 24 24 19 30 16 39 16 21 5 19 28 23 31 21 26 31 31 11 1 12 11 15 6 22 21 27 14
26	1	0	1 7 13 19 25 31 6 12 18 24 30 5 11 17 23 29 4 13 16 22 26 3 9 15 21 27 2 8 14 20 26 1 29 26 7 20 19 13 23 8 21 6 10 25 6 14 8 15 1 16 12 11 21 13 20 18 22 11 26 27 29 15
27	0	1	1 6 11 16 21 26 31 5 19 15 21 25 30 4 14 19 21 29 3 13 15 23 28 2 12 17 22 27 1 28 24 4 16 14 7 16 31 12 27 30 13 24 31 24 30 10 23 21 28 31 23 28 25 29 16 30 30 31 15
28	1	1	1 5 9 13 17 21 25 29 2 6 13 14 18 22 26 30 3 7 11 15 19 23 27 31 4 9 12 16 20 24 28 1 27 22 1 12 9 1 9 23 3 17 19 1 11 17 9 14 1 13 5 2 10 6 5 1 3 21 3 2 2 11
29	1	0	1 4 1 10 13 16 19 22 25 28 31 3 9 2 12 15 19 21 2 27 30 2 5 9 11 14 17 20 23 26 29 1 26 20 29 8 4 26 2 15 25 1 8 20 29 3 25 29 18 1 7 13 2 15 13 8 9 26 7 5 4 13
30	0	1	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 2 1 6 8 10 12 14 16 18 20 22 24 26 28 30 1 25 18 26 4 30 20 25 7 16 28 28 3 15 20 10 13 28 31 29 24 30 23 21 15 15 31 11 6 19
31	1	1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 20 21 22 23 24 25 26 27 28 29 30 31 1 24 16 23 31 25 14 19 30 7 18 17 27 3 6 26 2 19 13 10 4 9 2 29 22 21 5 15 11 9 20

For serial number  $i$ , the input sequence is  $u(t) = u(t)$  and the output sequence is  $y(t) = y(t)$ , where,  $u(t)$  is  $10000000000000000000000000000000, 10, \dots$  and  $y(t)$  is  $1011011011011011011011011011, 10, \dots$

Mapping of elements: 0 ----> 0 and  $i+1$  ---->  $a_i$ ,  $i=0, 1, 2, \dots, 30$ .

- (iv) Input and output period 15
- (v) Input and output period 31
- (vi) Input period 3/5, output period 15.

(a) Extension field  $GF(2^2)$ : The eigenvalues and corresponding unique states are listed in Table 4.9.

Table 4.9 Eigenvalues and Unique States in  $GF(2^2)$ ;  
 $c(x) = x^3 + x + 1$

e	x <sub>e</sub>			s(e)
	x <sub>1</sub>	x <sub>2</sub>	x <sub>3</sub>	
1	1	1	1	1
$\alpha$	$\alpha$	1	$\alpha^2$	$\alpha^2$
$\alpha^2$	$\alpha^2$	1	$\alpha$	$\alpha$

The spectral coefficients at input and output for three basis functions, given as input when the scrambler is in critical state is listed in Table 4.10. From the table it can be seen that

$$(i) y_e = s(e) u_e$$

$$(ii) \sum_e u_e x(e) = x_c$$

From Section 3.9, it follows that in all cases where input and output periods are three, above two properties hold good. Note that the analysis for period 3 can be done in  $GF(2^4)$  also since  $GF(2^2) \subset GF(2^4)$ .

Table 4.10 Spectral Coefficients at Input and Output for Sequences of Period 3;  $c(x) = x^3 + x + 1$

Critical State $x_c$			Input/Output Sequence		Input/Output Spectral Coefficients	
$x_1$	$x_2$	$x_3$				
0	1	0	100,...	1	1	1
			010,...	1	$\alpha^2$	$\alpha$
-----			010,...	1	$\alpha^2$	$\alpha$
1	0	0	001,...	1	$\alpha$	$\alpha^2$
-----			001,...	1	$\alpha$	$\alpha^2$
0	0	1	100,...	1	1	1

(b) Eigensequences from  $GF(2^3)$ :

Eigenvalues for eigenfunctions in  $GF(2^3)$  and corresponding unique initial states are given in Table 4.11.

Table 4.11 Eigenvalues and Unique States in  $GF(2^3)$   
 $c(x) = x^3 + x + 1$

$e$	$x_e$			$S(e)$
	$x_1$	$x_2$	$x_3$	
1	1	1	1	1
$\alpha^3$	$\alpha^2$	$\alpha^6$	$\alpha^3$	$\alpha^5$
$\alpha^5$	$\alpha$	$\alpha^3$	$\alpha^5$	$\alpha^6$
$\alpha^6$	$\alpha^4$	$\alpha^5$	$\alpha^6$	$\alpha^3$

Note: Eigenvalues not defined for  $e = \alpha, \alpha^2$  and  $\alpha^4$ .

From Equation (4.23) we have basis function for the sequence space, any sequence from which results in output period of 7 irrespective of initial state. Any other sequence of period 7 outside this space gives rise to output period 14. Spectral coefficients for these basis functions at input and at output when the initial state is zero is listed in Table 4.12. In the last row of the table is given, spectral coefficients for the zero input response when initial state is 001. Since for other initial states, zero input response is some shifted version of the same, spectral coefficients exist exactly at the same locations, but their coefficients are different.

Table 4.12 Spectral Coefficients at Input and Output for Sequences of Period 7;  $c(x) = x^3 + x + 1$

Initial State $x_c$			Input/Output Sequence	Input/Output Spectral Coefficients for $e =$					
$x_1$	$x_2$	$x_3$		1	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$
0	0	0	1111111,...	1	0	0	0	0	0
			1101000,...	1	$\alpha$	$\alpha^2$	0	$\alpha^4$	0
-----			-----						
0	0	0	1110100,...	0	0	0	1	0	1
			1100000,...	0	$\alpha^2$	$\alpha^4$	$\alpha^5$	$\alpha$	$\alpha^6$
-----			-----						
0	0	0	0111010,...	0	0	0	$\alpha^4$	0	$\alpha^2$
			0110000,...	0	$\alpha$	$\alpha^2$	$\alpha^2$	$\alpha^4$	$\alpha$
-----			-----						
0	0	0	0011101,...	0	0	0	$\alpha$	0	$\alpha^4$
			0011000,...	0	1	1	$\alpha^6$	1	$\alpha^3$
-----			-----						
0	0	1	0000000,...	0	0	0	0	0	0
			1011100,...	0	$\alpha^3$	$\alpha^6$	0	$\alpha^5$	0

From Table 4.12 and linearity of the scrambler it follows that for any sequence of period 7 and giving rise to output period 7,

- (i)  $y_e = u_e s(e)$ ,  $e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$
- (ii) Spectral coefficients at locations where eigenvalues are not defined are zero at the input side.
- (iii)  $\sum_e u_e x(e) + x_a$  generates sequences which give rise to new spectral coefficients at the output, at locations where eigenvalues are not defined.

(c) Eigenfunctions from  $GF(2^4)$ : Eigenvalues and corresponding unique states for all eigenfunctions in  $GF(2^4)$  are listed in Table 4.13. Let us first consider the case of input and output sequence both having periodicity 5. In Table 4.14 we have listed the spectral coefficients for five basis functions at input and at output when the scrambler is in critical state. In all cases, it can be seen that

$$(i) y_e = u_e s(e), \text{ for all } e$$

$$(ii) \sum_e u_e x(e) = x_c$$

This has to be so otherwise the period will be  $LCM(5, 7)$ , i.e. 35.

From Section 3.9 it follows that the above two properties are satisfied in all cases where the input sequence of period 5 results in output sequence of period 5 itself.

Now let us consider an input sequence of period 15 and giving rise to output period of 15 itself. Table 4.15 gives the spectral coefficients of 15 basis input sequences and

Table 4.13      Eigenvalues and Unique States in  $GF(2^4)$ ;  
 $c(x) = x^3 + x + 1$

e	x(e)			s(e)
	$x_1$	$x_2$	$x_3$	
1	1	1	1	1
$\alpha$	$\alpha^{10}$	$\alpha^9$	$\alpha^8$	$\alpha^{11}$
$\alpha^2$	$\alpha^5$	$\alpha^3$	$\alpha$	$\alpha^7$
$\alpha^3$	$\alpha^2$	$\alpha^{14}$	$\alpha^{11}$	$\alpha^5$
$\alpha^4$	$\alpha^{10}$	$\alpha^6$	$\alpha^2$	$\alpha^{14}$
$\alpha^5$	$\alpha^5$	1	$\alpha^{10}$	$\alpha^{10}$
$\alpha^6$	$\alpha^4$	$\alpha^{13}$	$\alpha^7$	$\alpha^{10}$
$\alpha^7$	$\alpha^9$	$\alpha^2$	$\alpha^{10}$	$\alpha$
$\alpha^8$	$\alpha^5$	$\alpha^{12}$	$\alpha^4$	$\alpha^{13}$
$\alpha^9$	$\alpha$	$\alpha^7$	$\alpha^{13}$	$\alpha^{10}$
$\alpha^{10}$	$\alpha^{10}$	1	$\alpha^5$	$\alpha^5$
$\alpha^{11}$	$\alpha^{12}$	$\alpha$	$\alpha^5$	$\alpha^8$
$\alpha^{12}$	$\alpha^8$	$\alpha^{11}$	$\alpha^{14}$	$\alpha^5$
$\alpha^{13}$	$\alpha^6$	$\alpha^8$	$\alpha^{10}$	$\alpha^4$
$\alpha^{14}$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^2$

of the resulting output sequences when the scrambler is in critical state. It can be seen that in each case

$$(i) \quad x_e = s(e) u_e, \quad \text{for all } e$$

$$(ii) \quad \sum_e u_e x(e) = x_c.$$

This has to happen otherwise period will be  $LCM(15,7)$ , i.e. 105.

Table 4.14 Spectral Coefficients at Input and Output for Sequence of Period 5;  $c(x) = x^3 + x + 1$

Critical States $x_c$	Input/Output Sequences	Input/Output Spectral Coefficients*
100	10000, ... 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0	
	11001, ... 1 0 0 6 0 0 11 0 0 11 0 0 6 0 0	
001	01000, ... 1 0 0 13 0 0 10 0 0 7 0 0 4 0 0	
	11100, ... 1 0 0 3 0 0 5 0 0 3 0 0 9 0 0	
011	00100, ... 1 0 0 10 0 0 4 0 0 13 0 0 7 0 0	
	01110, ... 1 0 0 15 0 0 14 0 0 8 0 0 12 0 0	
111	00010, ... 1 0 0 7 0 0 13 0 0 4 0 0 10 0 0	
	00111, ... 1 0 0 12 0 0 8 0 0 14 0 0 15 0 0	
110	00001, ... 1 0 0 4 0 0 7 0 0 10 0 0 13 0 0	
	10011, ... 1 0 0 9 0 0 2 0 0 5 0 0 3 0 0	

\*Mapping of elements as in Table 4.5.

Table 4.15 Spectral Coefficients at Input and Output for Sequence of Period 15;  
 $c(x) = x^3 + x + 1$

Critical States $x_c$	Input/Output Sequences	Input/Output Spectral Coefficients*
111	1000000000000000, ... 100101110010111, ...	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
110	0100000000000000, ... 110010111001011, ...	1 15 14 13 12 11 10 9 8 7 6 5 4 3 2
101	0010000000000000, ... 111001011100101, ...	1 14 12 10 8 6 4 2 15 13 11 9 7 5 3
010	0001000000000000, ... 111100101110010, ...	1 13 10 7 4 1 13 10 7 4 1 13 10 7 4
100	0000100000000000, ... 01110010111001, ...	1 12 8 4 15 11 7 3 14 10 6 2 13 9 5
001	0000010000000000, ... 10111001011100, ...	1 11 6 1 11 6 1 11 6 1 11 6 1 11 6
011	0000001000000000, ... 010111100101110, ...	1 10 4 13 7 1 10 4 13 7 1 10 4 13 7
111	0000000100000000, ... 001011110010111, ...	1 9 3 6 11 5 5 11 2 6 3 9 2 9
110	0000000010000000, ... 100101111001011, ...	1 8 15 9 14 6 2 4 12 5 11 10 3 13 7
101	0000000001000000, ... 110010111100101, ...	1 7 13 6 10 1 11 12 4 11 1 14 6 15 8
010	0000000000100000, ... 111001011110010, ...	1 6 11 3 6 11 5 5 11 2 6 3 9 2 9

continued...

Table 4.15 (continued)

Critical States $X_C$	Input/Output Sequences	Input/Output Spectral Coefficients*
100	00000000001000, ... 01100010111001, ...	1 5 9 13 2 6 10 14 3 7 11 15 4 8 12 1 1 3 1 5 15 1 2 1 8 9 12 14
001	00000000000100, ... 10110001011100, ...	1 4 7 10 13 1 4 7 10 13 1 4 7 10 13 1 15 14 15 12 11 14 8 8 6 12 12 14 15
011	00000000000010, ... 01011000101110, ...	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 1 14 12 12 8 6 8 1 15 14 11 1 15 1 1
111	00000000000001, ... 001011000101111, ...	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 1 13 10 9 4 1 2 9 7 5 1 5 3 3 2

\* Table should be read with following mapping for input/output spectral coefficients column  
 $i + 1 \rightarrow \alpha^i$   
 $i = 0, 1, \dots, 14$

From Section 3.9, it follows that in all cases where an input sequence of period 15 giving rise to output period 15, the above two conditions are satisfied. The case of input period 3/5 and output period 3/5 is also covered in this.

(b) Eigensequences from  $GF(2^5)$ : Eigenvalues and unique states for all eigensequences are given in Table 4.16. We will consider the case of input and output sequences having period 31. The spectral coefficients for 31 basis functions at input and for the resulting output sequences when the scrambler is in critical state are given in Table 4.17. It can be seen that

$$(i) \quad Y_e = U_e S(e), \quad \text{for all } e$$

$$(ii) \quad \sum_e U_e X(e) = X_c$$

in each case. From Section 3.9 it follows that any sequence of input period 31 resulting in a sequence of output period 31 satisfies the conditions (i) and (ii).

Exactly similar properties are observed in the case of the three stage scrambler having characteristic polynomial  $C(x) = x^3 + x^2 + 1$ . This can be verified from Tables B.1 to B.6 (Appendix B). Since the cases of input periods 3 and 5 resulting in output periods of 3 and 5 respectively are covered in the case of input and output period 15, separate tables for those cases are not attached.

5

Table 4.7 \* Eigenvalues and Unique States In GF(2<sup>5</sup>)  
2-Stage Scrambler.

e	X(e)		S(e)
	X <sub>1</sub>	X <sub>2</sub>	
1	1	1	1
2	22	21	23
3	12	10	14
4	17	14	20
5	23	19	27
6	15	10	20
7	2	27	8
8	5	29	12
9	14	6	22
10	20	11	29
11	29	19	8
12	26	15	6
13	3	22	15
14	8	26	21
15	9	26	23
16	27	12	11
17	27	11	12
18	9	23	26
19	8	21	26
20	3	15	22
21	26	6	15
22	29	8	19
23	20	29	11
24	14	22	6
25	5	12	29
26	2	8	27
27	15	20	10
28	23	27	19
29	17	20	14
30	12	11	10
31	22	23	21

Table 4.8 Spectral Coefficients at Input and Output for Sequences of Period 31:  $c(k) = x^2 + x + 1$ 

SI No	Initial State	Input/Output Spectral Coefficients																																			
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
2	1	0	1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2				
3	0	1	1	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2	31	29	27	25	23	21	19	17	15	13	11	9	7	5	3	2			
4	1	1	1	29	26	23	20	17	14	11	8	5	2	30	27	24	21	18	15	12	9	6	3	31	28	25	22	19	16	13	10	7	4				
5	1	0	1	28	24	20	16	12	8	4	31	27	23	19	15	11	7	3	30	26	22	18	14	10	6	2	29	25	21	17	13	9	5				
6	0	1	1	27	22	17	12	7	2	28	23	18	13	8	3	29	24	19	14	9	4	30	25	20	15	10	5	31	26	21	16	11	6				
7	1	1	1	26	20	14	8	2	27	21	15	9	3	28	22	16	10	4	29	23	17	11	5	30	24	18	12	6	31	25	19	13	7				
8	1	0	1	25	18	11	4	28	21	14	7	31	24	17	10	3	27	20	13	6	30	23	16	9	2	25	19	12	5	29	22	15	8				
9	0	1	1	24	16	8	31	23	15	7	30	22	14	6	29	21	13	5	28	20	12	4	27	19	11	3	26	18	10	2	25	17	9				
10	1	1	1	23	14	5	27	18	9	31	22	13	4	26	17	8	30	21	12	3	25	16	7	29	20	11	2	24	15	6	28	19	10				
11	1	0	1	22	12	2	23	13	3	24	14	4	25	15	5	26	16	6	27	17	7	28	18	8	29	19	9	30	20	10	31	21	11				
12	0	1	1	21	10	30	19	8	28	17	6	26	15	4	24	13	2	22	11	31	20	9	29	18	7	27	16	5	25	14	3	23	12	1	1		
13	1	1	1	20	8	27	15	3	22	10	29	17	5	24	12	31	19	7	26	14	2	21	9	28	16	4	23	11	30	18	6	25	13	2			
14	1	0	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14				
15	0	1	1	18	4	21	7	24	10	27	13	30	16	2	19	5	22	8	25	11	28	14	31	17	3	20	6	23	9	26	12	29	15	7	4		
16	1	1	1	17	2	18	3	19	4	20	5	21	6	22	7	23	8	24	9	25	10	26	11	27	12	28	13	29	14	30	15	31	16	5			
17	1	0	1	16	31	15	30	14	29	13	28	12	27	11	26	10	25	9	24	8	23	7	22	6	21	5	20	4	19	3	18	2	17				
18	0	1	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18				
19	1	1	1	14	27	9	22	4	17	30	12	25	7	20	2	15	28	10	23	5	18	31	13	26	8	21	3	16	29	11	24	6	19				
20	1	0	1	13	25	6	18	30	11	23	4	16	28	9	21	2	14	26	7	19	31	12	24	5	17	29	10	22	3	15	27	9	20				
21	0	1	1	12	23	3	14	25	5	16	27	7	18	29	9	20	31	11	22	2	13	24	4	15	26	6	17	29	8	19	30	10	21				

(contd.)

(Table 4.8 contd)

S1 Initial No State		Input/Output Spectral Coefficients																																
22	1	1	1	11	21	31	10	20	30	9	19	29	8	18	28	7	17	27	6	16	26	5	15	25	4	14	24	3	13	23	2	12	22	
				1	2	3	19	5	8	6	20	9	26	15	23	11	27	8	6	17	10	20	26	29	12	14	19	21	29	22	10	15	21	11
23	1	0	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22	31	9	18	27	5	14	23	
				1	1	1	16	1	3	31	13	1	17	5	12	30	14	25	22	1	24	2	7	9	22	23	27	28	4	27	14	18	23	12
24	0	1	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23	31	8	16	24	
				1	31	30	13	28	29	25	6	24	8	26	1	18	1	11	7	16	7	15	19	20	1	4	4	10	1	18	21	25	13	
25	1	1	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24	31	7	14	21	28	4	11	18	25	
				1	30	28	10	24	24	19	30	16	30	16	21	6	19	28	23	31	21	28	31	31	11	10	12	11	16	6	22	24	27	14
26	1	0	1	7	13	19	25	31	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	29	
				1	29	26	7	20	19	13	23	8	21	6	10	25	6	14	8	15	4	10	12	11	21	19	20	18	22	11	26	27	29	15
27	0	1	1	6	11	16	21	26	31	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27	
				1	28	24	4	16	14	7	16	31	12	27	30	13	24	31	24	30	18	23	24	22	31	28	28	25	28	16	30	30	31	16
28	1	1	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27	31	4	8	12	16	20	24	28	
				1	27	22	1	12	9	1	9	23	3	17	19	1	11	17	9	14	1	5	5	2	10	6	5	1	3	21	3	2	2	17
29	1	0	1	4	7	10	13	16	19	22	25	28	31	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	26	29	
				1	26	20	29	8	4	26	2	15	25	7	8	20	29	3	25	29	15	18	17	13	20	15	13	8	9	26	7	5	4	18
30	0	1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	
				1	25	18	26	4	30	20	26	7	16	28	28	8	16	20	10	13	29	31	29	24	30	24	21	15	15	31	11	8	6	19
31	1	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
				1	24	16	23	31	25	14	19	30	7	18	17	27	3	6	26	28	12	13	10	4	9	2	29	22	21	5	15	11	9	20

Mapping of elements:  $0 \rightarrow 0$  and  $i+1 \rightarrow a^i$ ,  $i=0,1,2,\dots,30$ .

- (iv) Input and output period 15
- (v) Input and output period 31
- (vi) Input period 3/5, output period 15.

(a) Extension field  $GF(2^2)$ : The eigenvalues and corresponding unique states are listed in Table 4.9.

Table 4.9 Eigenvalues and Unique States in  $GF(2^2)$ ;  
 $c(x) = x^3 + x + 1$

e	x <sub>e</sub>			s(e)
	x <sub>1</sub>	x <sub>2</sub>	x <sub>3</sub>	
1	1	1	1	1
$\alpha$	$\alpha$	1	$\alpha^2$	$\alpha^2$
$\alpha^2$	$\alpha^2$	1	$\alpha$	$\alpha$

The spectral coefficients at input and output for three basis functions, given as input when the scrambler is in critical state is listed in Table 4.10. From the table it can be seen that

$$(i) \quad y_e = s(e) u_e$$

$$(ii) \quad \sum_e u_e x(e) = x_c$$

From Section 3.9, it follows that in all cases where input and output periods are three, above two properties hold good. Note that the analysis for period 3 can be done in  $GF(2^4)$  also since  $GF(2^2) \subset GF(2^4)$ .

Table 4.10 Spectral Coefficients at Input and Output for Sequences of Period 3;  $c(x) = x^3 + x + 1$

Critical State $x_c$			Input/Output Sequence	Input/Output Spectral Coefficients		
$x_1$	$x_2$	$x_3$		$1$	$1$	$1$
0	1	0	100,...	1	1	1
			010,...	1	$\alpha^2$	$\alpha$
1	0	0	010,...	1	$\alpha^2$	$\alpha$
			001,...	1	$\alpha$	$\alpha^2$
0	0	1	001,...	1	$\alpha$	$\alpha^2$
			100,...	1	1	1

(b) Eigensequences from  $GF(2^3)$ :

Eigenvalues for eigenfunctions in  $GF(2^3)$  and corresponding unique initial states are given in Table 4.11.

Table 4.11 Eigenvalues and Unique States in  $GF(2^3)$   
 $c(x) = x^3 + x + 1$

$e$	Input/Output Sequence			$s(e)$
	$x_1$	$x_2$	$x_3$	
1	1	1	1	1
$\alpha^3$	$\alpha^2$	$\alpha^6$	$\alpha^3$	$\alpha^5$
$\alpha^5$	$\alpha$	$\alpha^3$	$\alpha^5$	$\alpha^6$
$\alpha^6$	$\alpha^4$	$\alpha^5$	$\alpha^6$	$\alpha^3$

Note: Eigenvalues not defined for  $e = \alpha, \alpha^2$  and  $\alpha^4$ .

From Equation (4.23) we have basis function for the sequence space, any sequence from which results in output period of 7 irrespective of initial state. Any other sequence of period 7 outside this space gives rise to output period 14. Spectral coefficients for these basis functions at input and at output when the initial state is zero is listed in Table 4.12. In the last row of the table is given, spectral coefficients for the zero input response when initial state is 001. Since for other initial states, zero input response is some shifted version of the same, spectral coefficients exist exactly at the same locations, but their coefficients are different.

Table 4.12 Spectral Coefficients at Input and Output for Sequences of Period 7;  $c(x) = x^3 + x + 1$

Initial State $x_c$			Input/Output Sequence	Input/Output Spectral Coefficients for $e =$					
$x_1$	$x_2$	$x_3$		1	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$
0	0	0	1111111,...	1	0	0	0	0	0
			1101000,...	1	$\alpha$	$\alpha^2$	0	$\alpha^4$	0
-----									
0	0	0	1110100,...	0	0	0	1	0	1
			1100000,...	0	$\alpha^2$	$\alpha^4$	$\alpha^5$	$\alpha$	$\alpha^6$
-----									
0	0	0	0111010,...	0	0	0	$\alpha^4$	0	$\alpha^2$
			0110000,...	0	$\alpha$	$\alpha^2$	$\alpha^4$	$\alpha$	$\alpha^4$
-----									
0	0	0	0011101,...	0	0	0	$\alpha$	0	$\alpha^4$
			0011000,...	0	1	1	$\alpha^6$	1	$\alpha^3$
-----									
0	0	1	0000000,...	0	0	0	0	0	0
			1011100,...	0	$\alpha^3$	$\alpha^6$	0	$\alpha^5$	0

From Table 4.12 and linearity of the scrambler it follows that for any sequence of period 7 and giving rise to output period 7,

- (i)  $Y_e = U_e S(e)$ ,  $e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$
- (ii) Spectral coefficients at locations where eigenvalues are not defined are zero at the input side.
- (iii)  $\sum_e U_e X(e) + X_a$  generates sequences which give rise to new spectral coefficients at the output, at locations where eigenvalues are not defined.

(c) Eigenfunctions from  $GF(2^4)$ : Eigenvalues and corresponding unique states for all eigenfunctions in  $GF(2^4)$  are listed in Table 4.13. Let us first consider the case of input and output sequence both having periodicity 5. In Table 4.14 we have listed the spectral coefficients for five basis functions at input and at output when the scrambler is in critical state. In all cases, it can be seen that

$$(i) Y_e = U_e S(e), \text{ for all } e$$

$$(ii) \sum_e U_e X(e) = X_c$$

This has to be so otherwise the period will be LCM (5, 7), i.e. 35.

From Section 3.9 it follows that the above two properties are satisfied in all cases where the input sequence of period 5 results in output sequence of period 5 itself.

Now let us consider an input sequence of period 15 and giving rise to output period of 15 itself. Table 4.15 gives the spectral coefficients of 15 basis input sequences and

Table 4.13 Eigenvalues and Unique States in  $GF(2^4)$ ;  
 $c(x) = x^3 + x + 1$

e	x(e)			s(e)
	$x_1$	$x_2$	$x_3$	
1	1	1	1	1
$\alpha$	$\alpha^{10}$	$\alpha^9$	$\alpha^8$	$\alpha^{11}$
$\alpha^2$	$\alpha^5$	$\alpha^3$	$\alpha$	$\alpha^7$
$\alpha^3$	$\alpha^2$	$\alpha^{14}$	$\alpha^{11}$	$\alpha^5$
$\alpha^4$	$\alpha^{10}$	$\alpha^6$	$\alpha^2$	$\alpha^{14}$
$\alpha^5$	$\alpha^5$	1	$\alpha^{10}$	$\alpha^{10}$
$\alpha^6$	$\alpha^4$	$\alpha^{13}$	$\alpha^7$	$\alpha^{10}$
$\alpha^7$	$\alpha^9$	$\alpha^2$	$\alpha^{10}$	$\alpha$
$\alpha^8$	$\alpha^5$	$\alpha^{12}$	$\alpha^4$	$\alpha^{13}$
$\alpha^9$	$\alpha$	$\alpha^7$	$\alpha^{13}$	$\alpha^{10}$
$\alpha^{10}$	$\alpha^{10}$	1	$\alpha^5$	$\alpha^5$
$\alpha^{11}$	$\alpha^{12}$	$\alpha$	$\alpha^5$	$\alpha^8$
$\alpha^{12}$	$\alpha^8$	$\alpha^{11}$	$\alpha^{14}$	$\alpha^5$
$\alpha^{13}$	$\alpha^6$	$\alpha^8$	$\alpha^{10}$	$\alpha^4$
$\alpha^{14}$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^2$

of the resulting output sequences when the scrambler is in critical state. It can be seen that in each case

$$(i) \quad y_e = s(e) u_e, \quad \text{for all } e$$

$$(ii) \quad \sum_e u_e x(e) = x_c.$$

This has to happen otherwise period will be  $LCM(15,7)$ , i.e. 105.

Table 4.14 Spectral Coefficients at Input and Output for Sequence of Period 5;  $c(x) = x^3 + x + 1$

Critical States $x_c$	Input/Output Sequences	Input/Output Spectral Coefficients*
100	10000, ... 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0	
	11001, ... 1 0 0 6 0 0 11 0 0 11 0 0 6 0 0	
001	01000, ... 1 0 0 13 0 0 10 0 0 7 0 0 4 0 0	
	11100, ... 1 0 0 3 0 0 5 0 0 3 0 0 9 0 0	
011	00100, ... 1 0 0 10 0 0 4 0 0 13 0 0 7 0 0	
	01110, ... 1 0 0 15 0 0 14 0 0 8 0 0 12 0 0	
111	00010, ... 1 0 0 7 0 0 13 0 0 4 0 0 10 0 0	
	00111, ... 1 0 0 12 0 0 8 0 0 14 0 0 15 0 0	
110	00001, ... 1 0 0 4 0 0 7 0 0 10 0 0 13 0 0	
	10011, ... 1 0 0 9 0 0 2 0 0 5 0 0 3 0 0	

\*Mapping of elements as in Table 4.5.

Table 4.15 Spectral Coefficients at Input and Output for Sequence of Period 15;  
 $c(x) = x^3 + x + 1$

Critical States $x_C$	Input/Output Sequences	Input/Output Spectral Coefficients*
111	10000000000000, ... 10010110010111, ...	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
110	01000000000000, ... 11001011001011, ...	1 12 8 6 15 11 11 2 14 11 6 9 6 5 3
101	00100000000000, ... 111001011100101, ...	1 15 14 13 12 11 10 9 8 7 6 5 4 3 2
010	00010000000000, ... 1110010111001010, ...	1 11 6 3 11 6 5 10 6 2 11 13 9 7 4
100	00001000000000, ... 00001000000000, ... 01110010111001, ...	1 14 12 10 8 6 4 2 15 13 11 9 7 5 3
001	00000100000000, ... 00000100000000, ... 010110010010100, ...	1 10 4 15 7 1 14 3 13 8 1 2 12 9 5
011	00000010000000, ... 00000010000000, ... 0101110010111001, ...	1 13 10 7 4 1 13 10 7 4 1 13 10 7 4
111	10000000000000, ... 10010110010111, ...	1 9 2 12 3 11 8 11 5 14 6 6 15 11 6
110	00000100000000, ... 01110010111001, ...	1 12 8 4 15 11 7 3 14 10 6 6 2 13 9 5
001	00000010000000, ... 010110010101100, ...	1 11 6 1 11 6 1 11 6 1 11 6 1 14 6 15 8
011	00000001000000, ... 01011100101110, ...	1 10 4 13 7 1 10 4 13 7 1 10 4 13 7
111	00000000100000, ... 00101110010111, ...	1 6 11 3 6 11 5 5 11 2 6 3 9 2 9
110	0000000001000000, ... 10010111001011, ...	1 5 9 15 2 10 3 11 4 12 5 13 6 14 7 15 8
001	11001011110010101, ... 0000000000100000, ... 0111001011110010, ...	1 8 15 7 14 6 13 5 12 4 11 3 10 2 9
010	0000000000100000, ... 1110010101110010, ...	1 7 13 4 10 1 7 13 14 10 1 7 13 4 10

continued...

Table 4.15 (continued)

Critical States $X_C$	Input/Output Sequences	Input/Output Spectral Coefficients*
100	00000000001000, ... 011100101111001, ...	1 5 9 13 2 6 10 14 3 7 11 15 4 8 12 1 1 3 1 1 5 15 1 2 1 8 9 12 14
001	00000000000100, ... 10111001011100, ...	1 4 7 10 13 1 4 7 10 13 1 4 7 10 13
011	00000000000010, ... 01011100101110, ...	1 15 14 15 12 11 14 8 8 8 6 12 12 14 15
111	00000000000001, ... 001011100101111, ...	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 1 14 12 12 8 6 8 1 15 14 11 1 15 1 1

\* Table should be read with following mapping for input/output spectral coefficients column

$$1 + 1 \rightarrow \alpha^1$$

$$1 = 0, 1, \dots, 14$$

From Section 3.9, it follows that in all cases where an input sequence of period 15 giving rise to output period 15, the above two conditions are satisfied. The case of input period 3/5 and output period 3/5 is also covered in this.

(b) Eigensequences from  $GF(2^5)$ : Eigenvalues and unique states for all eigensequences are given in Table 4.16. We will consider the case of input and output sequences having period 31. The spectral coefficients for 31 basis functions at input and for the resulting output sequences when the scrambler is in critical state are given in Table 4.17. It can be seen that

$$(i) \quad y_e = u_e s(e), \quad \text{for all } e$$

$$(ii) \quad \sum_e u_e x(e) = x_c$$

in each case. From Section 3.9 it follows that any sequence of input period 31 resulting in a sequence of output period 31 satisfies the conditions (i) and (ii).

Exactly similar properties are observed in the case of the three stage scrambler having characteristic polynomial  $C(x) = x^3 + x^2 + 1$ . This can be verified from Tables B.1 to B.6 (Appendix B). Since the cases of input periods 3 and 5 resulting in output periods of 3 and 5 respectively are covered in the case of input and output period 15, separate tables for those cases are not attached.

Table 4.16 Eigenvalues and Unique States In  $GF(2^5)$   
 $c(x)=x^3+x+1$

e	X(e)			S(e)
	$\chi_1$	$\chi_2$	$\chi_3$	
1	1	1	1	1
2	7	6	5	8
3	13	11	9	15
4	21	18	15	24
5	25	21	17	29
6	26	21	16	31
7	10	4	29	16
8	7	31	24	14
9	18	10	2	26
10	15	6	28	24
11	20	10	31	30
12	22	11	31	2
13	19	7	26	31
14	23	10	28	5
15	13	30	16	27
16	13	29	14	28
17	4	19	3	20
18	11	25	8	28
19	29	11	24	16
20	4	16	28	23
21	8	19	30	29
22	27	6	16	17
23	12	21	30	3
24	7	15	23	30
25	6	13	20	30
26	18	24	30	12
27	14	19	24	9
28	4	8	12	31
29	25	28	31	22
30	18	20	22	16
31	25	26	27	24

Mapping of elements:  $v \mapsto 0; 1+i \mapsto a^i, i=0,1,2,\dots,31.$

Table 4.17 Spectral Coefficients at Input and Output for Sequences of Period 31;  $c(x) = x^3 + x + 1$

(cont'd.)

(Table 4.17 contd)

Sl No	critical State	Input/Output Spectral Coefficients																														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
22	0 1 0	1	11	21	31	10	20	30	9	19	29	8	18	28	7	17	27	6	16	26	5	15	25	4	14	24	3	13	23	2	12	22
		1	18	4	23	7	19	14	22	13	21	6	19	27	11	12	23	25	12	10	27	11	10	6	12	22	14	21	22	23	27	14
23	1 0 0	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22	31	9	18	27	5	14	23
		1	17	2	20	3	14	8	15	5	12	27	8	15	29	29	8	9	26	23	8	22	20	15	20	29	20	26	26	29	15	
24	0 0 1	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23	31	8	16	24
		1	16	31	17	30	9	2	8	28	3	17	28	3	16	15	24	24	9	5	20	2	30	24	28	5	26	31	30	29	31	16
25	0 1 1	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24	31	7	14	21	28	4	11	18	25
		1	15	29	14	26	4	27	1	20	25	7	17	22	3	1	9	8	23	18	1	13	9	2	5	12	1	5	3	1	2	17
26	1 1 1	1	7	13	19	25	31	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	26
		1	14	27	11	22	30	21	25	12	16	28	6	10	21	18	25	23	6	31	13	24	19	11	13	19	7	10	7	4	4	18
27	1 1 0	1	6	11	16	21	26	31	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27
		1	13	25	8	18	25	15	18	4	7	18	26	29	8	4	10	7	20	13	25	4	29	20	21	26	13	15	11	7	6	19
28	1 0 1	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27	31	4	8	12	16	20	24	28
		1	12	23	5	14	20	9	11	27	29	8	15	17	26	21	26	22	3	25	6	15	8	29	29	2	19	20	15	10	8	20
29	0 1 0	1	4	7	10	13	16	19	22	25	28	31	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	26	29
		1	11	21	2	10	15	3	4	19	20	29	4	5	13	7	11	6	17	8	18	26	18	7	6	9	25	25	19	13	10	21
30	1 0 0	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
		1	10	19	30	6	10	28	28	11	11	19	24	24	31	24	27	21	31	21	30	6	28	10	14	16	31	30	23	16	12	22
31	0 0 1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		1	9	17	27	2	5	22	21	3	2	9	13	12	18	10	12	5	14	3	11	17	7	25	22	23	6	4	27	19	14	23

Mapping of elements: 0 ----> 0 and 1+1 ---->  $a^i$ ,  $i=0,1,\dots,30$ .

#### 4.7.3 Four Stage Scramblers:

Let us now consider the four stage scrambler having characteristic polynomial  $C(x) = x^4 + x + 1$ . shown in Figure 4.6.

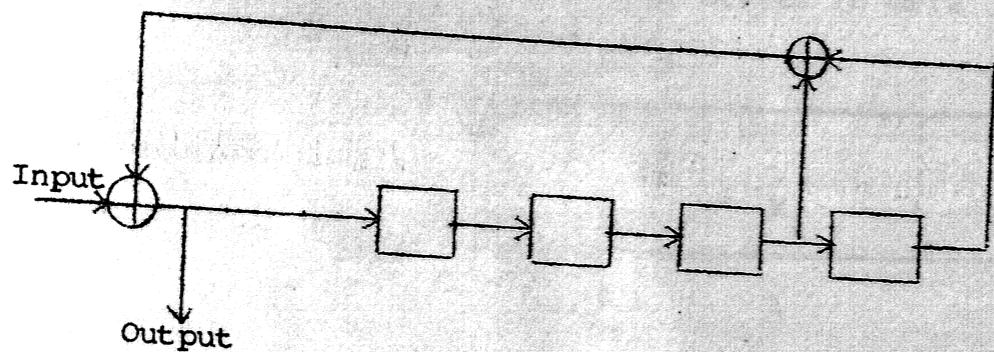


Figure 4.6 Four-stage Scrambler;  $c(x) = x^4 + x + 1$ .

In this case we will do spectral analysis which covers the following cases.

- (i) Input period 3 output period 3
- (ii) Input period 7 output period 7
- (iii) Input period 5 output period 5
- (iv) Input period 3/5 output period 15
- (v) Input period 15 output period 15
- (vi) Input period 31 output period 31.

(a) Exponent function from  $GF(2^2)$ : Eigenvalues and unique states for all eigensequences are given in Table 4.18. Table 4.19 gives input and output spectral coefficients for 3 basis sequences of period 3 and corresponding critical states. From Section 3.9 and these tables it follows that

$$(i) \quad x_e = u_e s(e) \text{ , for all } e$$

$$(ii) \quad \sum_e u_e x(e) = x_c ,$$

for any sequence of input and output periodicity 3. This is justified by Equation (4.50).

Table 4.18 Eigenvalues and Unique States in  $GF(2^2)$ ;  
 $c(x) = x^4 + x + 1$

$\epsilon$	X( $\epsilon$ )				$s(\epsilon)$
	$x_1$	$x_2$	$x_3$	$x_4$	
1	1	1	1	1	1
$\alpha$	1	$\alpha^2$	$\alpha$	1	$\alpha$
$\alpha^2$	1	$\alpha$	$\alpha^2$	1	$\alpha^2$

Table 4.19 Spectral Coefficients at Input and Output for Sequences of Period 3;  $c(x) = x^4 + x + 1$

Critical State $x_c$				Input/Output Sequences	Input/Output Spectral Coefficients		
$x_1$	$x_2$	$x_3$	$x_4$		1	$\alpha$	$\alpha^2$
1	0	0	1	100,...	1	1	1
				001,...	1	$\alpha$	$\alpha^2$
0	0	1	0	010,...	1	$\alpha^2$	$\alpha$
				100,...	1	1	1
0	1	0	0	001,...	1	$\alpha$	$\alpha^2$
				010,...	1	$\alpha^2$	$\alpha$

(b) Eigensequences from  $GF(2^3)$ : Eigenvalues and unique states for all eigensequences are given in Table 4.20. Input and output spectral coefficients of 7 basis functions of period 7 with their critical states are given in Table 4.21. From Section 3.9 and from the table it can be seen that

$$(i) \quad Y_e = U_e S(e) , \quad \text{for all } e$$

$$(ii) \quad \sum_e U_e X(e) = X_c ,$$

for any input sequence of period 7 and giving rise to a output sequence of period 7. This is justified by Equation (4.50).

(c) Eigensequences from  $GF(2^4)$ : The eigenvalues and corresponding unique states are listed in Table 4.22. Note that the eigenvalues are not defined for  $e = \alpha, \alpha^2, \alpha^4$  and  $\alpha^8$ .

Now let us consider the case of input and output periods of 5. The spectral coefficients at input and output for 5 basis functions of period 5, along with their critical states are listed in Table 4.23. From Section 3.9 and from this table it can be seen that

$$(i) \quad Y_e = U_e S(e) , \quad e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$$

$$(ii) \quad \sum_e U_e X(e) = X_c$$

for all the sequences of input and output periods 7. This is justified by Equation (4.50).

Now let us consider the case of input period 15 resulting in output period 15 irrespective of initial state. In Illustration 4.2 we have obtained a set of basis functions which spans the space

Table 4.20 Eigenvalues and Unique States in  $GF(2^3)$ ;  
 $c(x) = x^4 + x + 1$

e	x(e)				s(e)
	$x_1$	$x_2$	$x_3$	$x_4$	
1	1	1	1	1	1
$\alpha$	$\alpha^4$	$\alpha^3$	$\alpha^2$	$\alpha$	$\alpha^5$
$\alpha^2$	$\alpha$	$\alpha^6$	$\alpha^4$	$\alpha^2$	$\alpha^3$
$\alpha^3$	$\alpha^3$	1	$\alpha^4$	$\alpha$	$\alpha^6$
$\alpha^4$	$\alpha^2$	$\alpha^5$	$\alpha$	$\alpha^4$	$\alpha^6$
$\alpha^5$	$\alpha^5$	1	$\alpha^2$	$\alpha^4$	$\alpha^3$
$\alpha^6$	$\alpha^6$	1	$\alpha$	$\alpha^2$	$\alpha^5$

consisting of such sequences. The spectral coefficients at input and output for these basis functions when the scrambler is in zero state are listed in Table 4.24. The last row in the table gives the spectral coefficients of zero input response when the scrambler state is 0001. The zero input responses for other states have spectral contents similar, only coefficients being different. In each case it can be seen that

- (i)  $y_e = u_e s(e)$ ,  $e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$
- (ii) The spectral coefficients at input in those places where eigenvalue is not defined are zero.
- (iii) The new spectral coefficients appearing at output are due to the zero input response for the state  $x_T$  given by

$$x_T = \sum u_e x(e) + x_a$$

Table 4.21 Eigenvalues and Unique States in  $GF(2^3)$ ;  
 $c(x) = x^4 + x + 1$

Critical State $x_c$				Input/Output Sequences		Input/Output Spectral Coefficients					
$x_1$	$x_2$	$x_3$	$x_4$								
0	1	1	1	1000000,...	1	1	1	1	1	1	1
				1011110,...	1	$\alpha^5$	$\alpha^3$	$\alpha^6$	$\alpha^6$	$\alpha^3$	$\alpha^5$
---				-----							
1	1	1	1	0100000,...	1	$\alpha^6$	$\alpha^5$	$\alpha^4$	$\alpha^3$	$\alpha^2$	$\alpha$
				0101111,...	1	$\alpha^4$	$\alpha$	$\alpha^3$	$\alpha^2$	$\alpha^5$	$\alpha^6$
---				-----							
1	1	1	0	0010000,...	1	$\alpha^5$	$\alpha^3$	$\alpha$	$\alpha^6$	$\alpha^4$	$\alpha^2$
				1010111,...	1	$\alpha^3$	$\alpha^6$	1	$\alpha^5$	1	1
---				-----							
1	1	0	1	0001000,...	1	$\alpha^4$	$\alpha$	$\alpha^5$	$\alpha^2$	$\alpha^6$	$\alpha^3$
				1101011,...	1	$\alpha^2$	$\alpha^4$	$\alpha^4$	$\alpha$	$\alpha^2$	$\alpha$
---				-----							
1	0	1	0	0000100,...	1	$\alpha^3$	$\alpha^6$	$\alpha^2$	$\alpha^5$	$\alpha$	$\alpha^4$
				1110101,...	1	$\alpha$	$\alpha^2$	$\alpha$	$\alpha^4$	$\alpha^4$	$\alpha^2$
---				-----							
0	1	0	1	0000010,...	1	$\alpha^2$	$\alpha^4$	$\alpha^6$	$\alpha$	$\alpha^3$	$\alpha^5$
				1111010,...	1	1	1	$\alpha^5$	1	$\alpha^6$	$\alpha^3$
---				-----							
1	0	1	1	0000001,...	1	$\alpha$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$
				0111101,...	1	$\alpha^6$	$\alpha^5$	$\alpha^2$	$\alpha^3$	$\alpha$	$\alpha^4$

Table 4.22 Eigenvalues and Unique States in  $GF(2^4)$ ;  
 $c(x) = x^4 + x + 1$

e	x(e)				s(e)
	$x_1$	$x_2$	$x_3$	$x_4$	
1	1	1	1	1	1
$\alpha^3$	$\alpha^4$	$\alpha$	$\alpha^{13}$	$\alpha^{10}$	$\alpha^7$
$\alpha^5$	1	$\alpha^{10}$	$\alpha^5$	1	$\alpha^5$
$\alpha^6$	$\alpha^8$	$\alpha^2$	$\alpha^{11}$	$\alpha^5$	$\alpha^{14}$
$\alpha^7$	$\alpha^{11}$	$\alpha^4$	$\alpha^{12}$	$\alpha^5$	$\alpha^3$
$\alpha^9$	$\alpha^2$	$\alpha^8$	$\alpha^{14}$	$\alpha^5$	$\alpha^{11}$
$\alpha^{10}$	1	$\alpha^5$	$\alpha^{10}$	1	$\alpha^{10}$
$\alpha^{11}$	$\alpha^{13}$	$\alpha^2$	$\alpha^6$	$\alpha^{10}$	$\alpha^9$
$\alpha^{12}$	$\alpha$	$\alpha^4$	$\alpha^7$	$\alpha^{10}$	$\alpha^{13}$
$\alpha^{13}$	$\alpha^{14}$	$\alpha$	$\alpha^3$	$\alpha^5$	$\alpha^{12}$
$\alpha^{14}$	7	8	9	10	6

where  $x_a$  is the actual state and  $e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$ .

From the linearity of the scrambler it follows that the entire space of sequences having input and output periods 15 irrespective of initial state satisfies the conditions (i), (ii) and (iii).

Table 4.23\* Spectral Coefficients at Input and Output for Sequences of Period 5;  $c(x) = x^4 + x + 1$

Critical States $x_c$	Input/ Output Sequences	Input/Output Spectral Coefficients														
1101	10000, ...	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
	01011, ...	1	0	0	8	0	0	15	0	0	12	0	0	14	0	0
1010	01000, ...	1	0	0	13	0	0	10	0	0	7	0	0	4	0	0
	10101, ...	1	0	0	5	0	0	9	0	0	3	0	0	2	0	0
0101	00100, ...	1	0	0	10	0	0	4	0	0	13	0	0	7	0	0
	11010, ...	1	0	0	2	0	0	3	0	0	9	0	0	5	0	0
1011	00010, ...	1	0	0	7	0	0	13	0	0	4	0	0	10	0	0
	01101, ...	1	0	0	14	0	0	12	0	0	15	0	0	8	0	0
0110	00001, ...	1	0	0	4	0	0	7	0	0	10	0	0	13	0	0
	10110, ...	1	0	0	11	0	0	6	0	0	6	0	0	11	0	0

\* Mapping as in Table 4.5.

(d) Eigensequences from  $GF(2^5)$ : The eigenvalues with their corresponding unique states are given in Table B.7. The spectral coefficients at input and output for 31 basis functions along with their critical states are listed in Table B.8. From this table it can be seen that in each case

$$(i) \quad y_e = u_e s(e), \quad \text{for all } e$$

$$(ii) \quad \sum_e u_e x(e) = x_c$$

From Section 3.9 it follows that these two conditions are satisfied by any sequence of input and output periodicity 31.

Similar results are observed in the case of scrambler with  $c(x) = x^4 + x^3 + 1$ . This can be verified from corresponding

Tables B.9 to B.17.

\*  
Table 4.24 Spectral Coefficients at Input and Output  
for Sequences of Period 15;  $c(x) = x^4 + x + 1$

Sl. No.	Critical States	Input/Output	Spectral Coefficients
1	0000	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0
2/1	0000	0 0 0 0 0 6 0 11 11 0 0 0 6 0 11 0 0 0 0 0	0 11 6 0 11 11 0 0 0 6 0 11 0 0 0 0 0 0 0
2/2	0000	0 0 0 0 0 7 1 6 0 0 0 13 0 11 0 0 0 0 0 0	0 10 4 0 7 1 6 0 0 0 13 0 11 0 0 0 0 0 0
3/1	0000	0 0 0 12 5 0 8 0 0 8 10 0 0 15 0 0 0	0 2 3 4 5 0 7 0 0 8 10 0 0 13 0 0 0
3/2	0000	0 0 0 9 1 0 2 0 0 1 1 5 0 0 3 0 0 0	0 1 1 1 1 0 1 0 0 1 1 5 0 0 1 0 0 0
3/3	0000	0 0 0 6 12 0 0 11 0 0 8 7 0 0 6 0 0 0	0 15 14 13 12 0 0 10 0 0 8 7 0 0 4 0 0 0
3/4	0000	0 0 0 3 0 0 5 0 0 0 15 13 0 0 9 0 0 0	0 14 12 10 8 0 4 0 0 15 13 0 0 7 0 0 0
4/1	0000	0 0 0 0 0 0 0 8 0 0 11 15 0 0 12 0 14 15	0 14 12 0 8 0 0 0 11 15 0 0 12 0 14 15
4/2	0000	0 0 0 0 0 0 0 4 0 0 4 7 0 0 0 10 0 13 7	0 13 10 0 4 0 0 0 4 7 0 0 0 10 0 13 7
4/3	0000	0 0 0 0 0 0 0 9 0 0 12 14 0 0 0 5 0 3 2	0 12 8 0 15 0 0 0 12 14 0 0 0 14 0 15 0 3 2
4/4	0000	0 0 0 0 0 0 0 2 0 0 5 6 0 0 3 0 5 3	0 11 6 0 11 0 0 0 2 0 5 6 0 0 3 0 2 9
5	0001	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 4 7 0 13 0 0 0 10 0 0 0 0 0 0 0 0 0

\* Mapping is as follows:  $0 \rightarrow a_i, i=0, 1, 2, \dots, 14$ .  
Input for serial no  $i$  is  $\underbrace{11111111111111\dots}_{i-1}$

Input for serial no  $i/1$  is  $0 \quad u(i,t), j=2, 3, 4$  and  $i=1, 2, 3, 4$   
 $u(2,t)$  is  $110110110110110, \dots$   
 $u(3,t)$  is  $110001100011000, \dots$   
 $u(4,t)$  is  $111101011001000, \dots$

The last column gives spectral coefficients of the zero  
input response for the state  $0 \ 0 \ 0 \ 1$ .

The output sequence for serial no 1 is  $1010011011000, \dots$

#### 4.7.4 Five Stage Scramblers:

The five stage scrambler having the characteristic polynomial  $c(x) = x^5 + x^2 + 1$  is given in Figure 4.7. In this

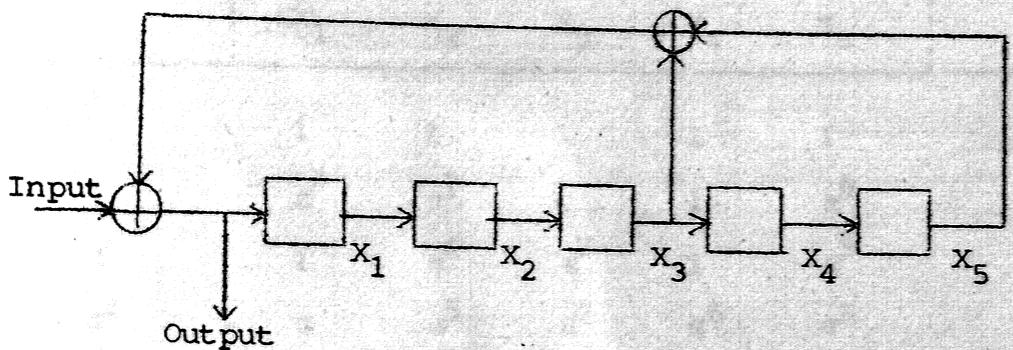


Figure 4.7 Five-stage Scrambler;  $c(x) = x^5 + x^2 + 1$ .

we will analyse the scrambler for the following cases.

- (i) Input period 7 output period 7
- (ii) Input periods 3, 5 and 15 giving rise to output periods 3, 5 and 15 respectively
- (iii) Input period 31 and output period 31.

(a) Eigensequences from  $GF(2^3)$ : The eigenvalues and their corresponding unique states are listed in Table 4.25. The spectral coefficients at input and at output for 7 basis functions of period 7 and their critical states are listed in Table 4.26. From this table and from Section 3.9 it follows that for any sequence of input and output periodicity 7,

$$(i) \quad y_e = u_e s(e) , \quad \text{for all } e$$

$$(ii) \quad \sum_e u_e x(e)' = x_c .$$

This is justified by Equation (4.50).

Table 4.25 Eigenvalues and Unique States in  $GF(2^3)$ ;  
 $c(x) = x^5 + x^2 + 1$

e	x(e)					s(e)
	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	
1	1	1	1	1	1	1
$\alpha$	$\alpha^3$	$\alpha^2$	$\alpha$	1	$\alpha^6$	$\alpha^4$
$\alpha^2$	1	$\alpha^4$	$\alpha^2$	1	$\alpha^5$	$\alpha$
$\alpha^3$	$\alpha$	$\alpha^5$	$\alpha^2$	$\alpha^6$	$\alpha^3$	$\alpha$
$\alpha^4$	$\alpha^5$	$\alpha$	$\alpha^4$	1	$\alpha^3$	$\alpha^2$
$\alpha^5$	$\alpha^4$	$\alpha^6$	$\alpha$	$\alpha^3$	$\alpha^5$	$\alpha^2$
$\alpha^6$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$	$\alpha$

Table 4.26. Spectral Coefficients at Input and Output for Sequence of Period 7;  $c(x) = x^5 + x^2 + 1$

Critical States $X_C$	Input/Output Sequences	Input/Output Spectral Coefficients							
00111	1000000, ...	1	1	1	1	1	1	1	
	1111100, ...	1	$\alpha^4$	$\alpha$	$\alpha^4$	$\alpha^2$	$\alpha^2$	$\alpha$	
0111	0100000, ...	1	$\alpha^6$	$\alpha^5$	$\alpha^4$	$\alpha^3$	$\alpha^2$	$\alpha$	
	0111110, ...	1	$\alpha^3$	$\alpha^6$	$\alpha$	$\alpha^5$	$\alpha^4$	$\alpha^2$	
11111	0010000, ...	1	$\alpha^5$	$\alpha^3$	$\alpha$	$\alpha^6$	$\alpha^4$	$\alpha^2$	
	0011111, ...	1	$\alpha^2$	$\alpha^4$	$\alpha^5$	$\alpha$	$\alpha^6$	$\alpha^3$	
11110	0001000, ...	1	$\alpha^4$	$\alpha$	$\alpha^5$	$\alpha^2$	$\alpha^6$	$\alpha^3$	
	1001111, ...	1	$\alpha$	$\alpha^2$	$\alpha^2$	$\alpha^4$	$\alpha$	$\alpha^4$	
11100	0000100, ...	1	$\alpha^3$	$\alpha^6$	$\alpha^2$	$\alpha^5$	$\alpha$	$\alpha^4$	
	1100111, ...	1	1	1	$\alpha^6$	1	$\alpha^3$	$\alpha^5$	
11001	0000010, ...	1	$\alpha^2$	$\alpha^4$	$\alpha^6$	$\alpha$	$\alpha^3$	$\alpha^5$	
	1110011, ...	1	$\alpha^6$	$\alpha^5$	$\alpha^3$	$\alpha^3$	$\alpha^5$	$\alpha^6$	
10011	0000001, ...	1	$\alpha$	$\alpha^2$	$\alpha^3$	$\alpha^4$	$\alpha^5$	$\alpha^6$	
	1111001, ...	1	$\alpha^5$	$\alpha^3$	1	$\alpha^6$	1	1	

(b) Eigensequences from  $GF(2^4)$ : The eigenvalues and corresponding unique states are listed in Table 4.27. The spectral coefficients at input and at output for 15 basis functions of period 15 and their critical states are listed in Table 4.28. From this table and from Section 3.9 it follows that for any sequence of input and output periodicity 15,

$$(i) \quad Y_e = U_e S(e) \quad , \quad \text{for all } e$$

$$(ii) \quad \sum_{e=1}^4 U_e X(e) = X_c$$

This is justified by Equation (4.50).

This covers the case of input and output periodicities 3 and 5 also.

(c) Eigensequences from  $GF(2^5)$ : Eigenvalues and corresponding unique states are listed in Table 4.29. The eigenvalues are not defined for  $e = \alpha, \alpha^2, \alpha^4, \alpha^8$  and  $\alpha^{16}$ . Let us now consider the case of input sequences of period 31 giving rise to output sequences of period 31 irrespective of initial state of the scrambler. Proceeding as in Illustration 4.1, a set of 26 basis functions which span the vector space consisting of such sequences are obtained. The spectral coefficients at input and at output for these basis functions when the scrambler is in zero state are listed in Table 4.30. The last row in the table gives the spectral coefficient of zero input response when the scrambler state is 00001. The zero input responses for other states have spectral contents similar, only coefficients are different.

In each case it can be seen that

Table 4.27\* Eigenvalues and Unique States in  $GF(2^4)$ ;  
 $c(x) = x^5 + x^2 + 1$

e	x(e)					s(e)
	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	
1	1	1	1	1	1	1
2	1	15	14	13	12	2
3	1	14	12	10	8	3
4	7	4	1	13	10	10
5	1	12	8	4	15	5
6	6	1	11	6	1	11
7	13	7	1	10	4	4
8	8	11	4	12	5	10
9	1	8	15	7	14	9
10	4	10	1	7	13	13
11	11	1	6	11	1	6
12	2	6	10	14	3	13
13	10	13	1	4	7	7
14	9	11	13	15	2	7
15	5	6	7	8	9	4

\* Mapping as in Table 4.6.

Table 4.28 Spectral Coefficients at Input and Output  
for Sequences of Period 15;  $c(x) = x^5 + x^2 + 1$

Critical States	Input/Output	Spectral Coefficients
11011		1 2 3 10 5 11 4 10 9 13 6 13 7 7 4
1110		1 15 14 13 12 11 10 9 8 7 6 13 3 1 4 11 5 2 10 4 3 5
01100		1 14 12 10 4 8 6 7 2 15 13 11 9 7 5 6 13 11 6
11000		1 13 10 7 4 1 13 10 7 4 15 1 6 13 10 1 13 7 4
10001		1 12 9 4 15 11 7 3 14 10 7 6 11 14 2 13 9 5 8
00011		1 11 8 10 15 6 1 4 11 5 14 13 1 11 3 7 11 2 6
00111		1 10 4 13 7 1 10 4 13 6 7 4 1 6 10 7 10 4 13 7 10
01111		1 9 2 10 4 7 11 6 7 12 5 13 10 11 14 13 7 15 6 11
11111		1 8 15 7 14 6 13 1 14 5 12 4 11 1 15 10 1 2 9
11110		1 7 13 4 10 1 7 13 4 10 7 6 7 13 4 10 4 10
11100		1 6 11 1 10 6 11 1 5 11 4 13 1 11 6 11 1 7 12 14
11001		1 5 9 13 2 6 1 10 14 3 7 11 4 1 12 10 14 8 12
10011		1 4 7 10 4 13 2 11 4 7 1 10 3 13 10 1 6 4 13 1 10 13
00110		1 3 5 7 1 13 6 11 13 15 2 4 1 6 8 10 12 3 14 2
01101		1 2 3 5 13 5 6 7 8 2 10 7 11 12 13 4 14 5 15

- (i)  $Y_e = U_e S(e)$ ,  $e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$
- (ii) The spectral coefficients at input in those places where eigenvalue is not defined are zero
- (iii) The new spectral coefficients appearing at output are due to the zero input response for the state  $X_T$  given by

$$X_T = \sum_e U_e X(e) + X_a$$

where  $X_a$  is the initial state of the scrambler.

From the linearity of the scrambler it follows that the entire space of sequences having input and output periods equal to 31 irrespective of initial state satisfies the conditions (i), (ii) and (iii).

Similar results are observed for other 5 structures of 5-stage scramblers. It can be verified from the corresponding Tables B.18 to B.23 for the scrambler with  $c(x) = x^5 + x^4 + x^2 + 1$ .

From the analysis carried out it is seen that

1. The eigenvalues are defined for all eigensequences over extension field  $GF(2^m)$  for a  $n$ -stage scrambler when  $n$  is not a divisor of  $m$ .
2. For a  $n$ -stage scrambler, eigenvalues for  $n$  eigensequences from  $GF(2^n)$  are not defined.
3. For input and output sequences of period not equal to the cycle length
  - (a)  $Y_e = U_e S(e)$ , for all  $e$ , and
  - (b)  $\sum_e U_e X(e) = X_c$
4. For input and output sequences of period equal to a multiple of cycle length,

Table 4.29\* Eigenvalues and corresponding Unique States  
 In  $GF(2^5)$ ;  $c(x) = x^5 + x^2 + 1$

e	X(e)					S(e)
	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	
1	1	1	1	1	1	1
4	6	3	31	28	25	9
6	23	18	13	8	3	28
7	11	5	30	24	18	17
8	9	2	26	19	12	16
10	22	13	4	26	17	31
11	14	4	25	15	5	24
12	8	18	17	6	26	19
13	21	9	28	16	4	2
14	29	16	3	21	8	11
15	17	3	20	6	23	31
16	7	23	8	24	9	22
18	19	2	16	30	13	5
19	12	25	7	20	2	30
20	5	17	29	10	22	24
21	27	7	18	29	9	16
22	20	30	9	19	29	10
23	15	24	2	11	20	6
24	4	12	20	28	5	27
25	10	17	24	31	7	3
26	3	9	15	21	27	28
27	26	31	5	10	15	21
28	18	22	26	30	3	14
29	2	5	8	11	14	30
30	25	27	29	31	2	23
31	13	14	15	16	17	12

For  $e=2, 3, 5, 9$ , and 17 Eigenvalue is not defined.

\* Mapping as in Table 4.8

Table 4.30 Spectral Coefficients at Input and Output for Sequences of Period 31;  $c(x) = x^5 + x^2 + 1$

S1 No	Initial State	Input/Output Spectral Coefficients																												
		1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	00000	1	15	29	0	26	0	0	0	20	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0
2/1	00000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	0	0	0	0	0	0	0	0	0
2/2	00000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	30	0	0	0	0	0	0	0	0	0	0	0	0
2/3	00000	0	16	31	0	30	0	0	0	28	0	0	0	0	0	0	0	20	24	0	0	0	0	0	0	0	0	0	0	0
2/4	00000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0	0	0	0	0	0
2/5	00000	0	14	27	0	22	0	0	0	12	0	0	0	0	0	0	0	21	23	0	0	0	0	0	0	0	0	0	0	0
3/1	00000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0	0
3/2	00000	0	13	25	0	18	0	0	0	4	0	0	0	0	0	0	0	6	7	0	0	0	0	0	0	0	0	0	0	0
3/3	00000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20	0	0	0	0	0	0	0	0	0	0	0	0
3/4	00000	0	11	21	0	10	0	0	0	19	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0
3/5	00000	0	10	19	0	6	0	0	0	11	0	0	0	0	0	0	0	27	0	0	0	0	0	0	0	0	0	0	0	0
4/1	00000	0	0	0	11	0	0	21	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0
4/2	00000	0	16	31	19	30	0	6	0	28	0	0	0	0	0	0	0	11	0	0	0	0	0	0	0	0	0	0	0	0
4/3	00000	0	0	0	8	0	0	15	0	0	0	0	0	0	0	0	29	0	0	0	0	0	0	0	0	0	0	0	0	0
4/4	00000	0	15	29	16	26	0	31	0	20	0	0	0	0	0	0	0	30	0	0	0	0	0	0	0	0	0	0	0	0
4/5	00000	0	0	0	5	0	0	9	0	0	0	0	0	0	0	0	17	0	0	0	0	0	0	0	0	0	0	0	0	0
4/6	00000	0	14	27	13	22	0	25	0	12	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0
4/7	00000	0	0	0	2	0	0	3	0	0	0	0	0	0	0	0	27	0	0	0	0	0	0	0	0	0	0	0	0	0
4/8	00000	0	13	25	10	18	0	19	0	4	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0
4/9	00000	0	0	0	30	0	0	28	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	0	0	0	0	0	0
4/10	00000	0	12	23	7	14	0	13	0	27	0	0	0	0	0	0	25	0	0	0	0	0	0	0	0	0	0	0	0	0
5/1	00000	0	0	0	0	0	0	0	23	0	0	0	0	0	0	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0
5/2	00000	0	31	30	0	28	0	0	7	24	0	0	0	0	0	0	0	13	0	16	0	0	4	0	0	0	0	0	0	0
5/3	00000	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	31	0	0	0	0	24	0	0	0	0	0	0	0
5/4	00000	0	29	26	0	20	0	0	0	24	8	0	0	0	0	0	0	17	0	0	0	0	5	0	0	0	0	0	0	0
5/5	00000	0	28	24	0	16	0	0	0	17	31	0	0	0	0	0	0	2	0	30	0	0	9	0	0	5	0	0	0	
5/6	00000	0	0	0	0	0	0	0	0	26	0	0	0	0	0	0	0	20	0	0	0	0	29	0	0	0	0	15	0	0
5/7	00000	0	27	22	0	12	0	0	0	10	23	0	0	0	0	0	0	19	0	14	0	0	21	0	0	0	0	11	0	0

(contd.)

(Table 4.30 contd)

Input for serial no 1 is 11111111111111111111111111111111

The last row gives spectral coefficients of the zero input response for the state 0 0 0 0 1.

Input for serial no  $j/i$  is  $D^{i-1} u(j,t)$  ,  $j=2,\dots,6$ . and  $i=1,2,\dots,5$ . where.

$$u(1,t)=1010111011000111110011010010000$$

$$u(2,t)=1101010010001011111011001110000$$

$$u(3,t)=110010011110111000101011010000$$

$$u(4,t)=101101010001110111100100110000$$

$$u(5,t)=111001101111010001001010110000$$

Output for serial no 1 is 111001000101011101101001100000

The zero input response for the state 0 0 0 1 is 100101100111100011011101010000...

Output for serial no  $j/i$  is  $D^{i-1} y(j,t)$  ,  $j=2,3,\dots,6$ , and  $i=1,\dots,5$ , where,

$$y(2,t)=1011110010110100111101000000000$$

$$y(3,t)=1100101110100010101011000000000$$

$$y(4,t)=1101010111100100101001000000000$$

$$y(5,t)=1010010010101101001111000000000$$

$$y(6,t)=1111111011010110010111000000000$$

Mapping of field elements as in Table 4.8

Digitized by srujanika@gmail.com

- (a)  $Y_e = U_e S(e), e \in \{e | \text{eigenvalue is defined for } \{e^k\}\}$
- (b) Spectral coefficients at input, of those eigensequences for which eigenvalues are not defined, are zero, and
- (c) The new coefficients which appear at the output are due to the zero input response of the scrambler for the state  $X_T$  given by

$$X_T = \sum_e U_e X(e) + X_a$$

where  $X_a$  is the actual initial state of the scrambler.

## CHAPTER 5

### CONCLUSION

In this chapter we summarize various results obtained and observations made in this thesis and make suggestions for further work in this area.

#### 5.1. Conclusion

The important results obtained concerning the periodic output of the scrambler when excited by a periodic input are:

1. If the periods of input sequence is not a multiple of the cycle length  $q$  of the scrambler, then but for a unique initial state of the scrambler for which the period remains unaltered, the period of the output sequence is  $\text{LCM}(s, q)$ .
2. If the period  $s$  of the input sequence is a multiple of the cycle length of the scrambler, say  $s$  is some  $rq$ , then the period of the output sequence is also a multiple of the cycle length i.e. the period is some  $r'q$  ( $r'$  not necessarily different from  $r$ ).
3. There is no advantage in scrambling a M-sequence of length equal to cycle length of the scrambler and generated by a structure different from that of the scrambler.

From the spectral analysis of scramblers, the important observations made are:

1. For a  $n$ -stage scrambler eigenvalues for  $n$  eigensequences over an extension field  $\text{GF}(2^n)$  are not defined. However,

eigenvalues are defined for all eigensequences over  $GF(2^m)$  when  $n$  is not a divisor of  $m$ .

2. For input and output sequences of period not equal to cycle length of the scrambler,

$$(a) \quad Y_e = U_e S(e) \quad \text{for all } e$$

$$\text{and (b)} \quad \sum_e U_e X(e) = X_c$$

3. For input and output sequences of period, a multiple of cycle length,

$$(a) \quad Y_e = U_e S(e), e \in \{e \mid \text{eigenvalue is defined for } \{e^k\}\}$$

(b) spectral coefficients at input, of those eigensequences for which eigenvalues are not defined, are zero,

and

(c) the new spectral coefficients which appear at the output are due to the zero input response of the scrambler for the state  $X_T$  given by

$$X_T = \sum_e U_e X(e) + X_a$$

where  $X_a$  is the initial state of the scrambler.

### 5.2. Suggestions for Further Research

Performance of scramblers defined over any modular field  $GF(p)$  in general can be studied using techniques similar to those employed in Chapter 3.

In this thesis spectral theory for LSCs defined over a modular field is used to carry out the spectral analysis of the

input and output sequences and observations as outlined in Section 5.1 are made based on this analysis. The analysis reported in the thesis holds good for input and output sequences with periodicities equal to  $2^n - 1$  or to a divisor of  $2^n - 1$  for some integer  $n$ . Further investigation may be carried out to see whether LSCs can be studied completely in a manner analogous to frequency domain analysis of continuous linear time-invariant systems. In other words whether it is possible to develop a theory similar to that of Fourier transform, by exploiting the concept of formal derivative discussed in Chapter 3.

REFERENCES

1. Arazi, B., Self Synchronising Digital Scramblers, IEEE Transactions on Communications, Vol. COM-25, No. 12, December 1977, pp. 1505-1507.
2. Booth, T.L., Sequential Machines and Automata Theory, John Wiley and Sons, Inc., 1967, pp. 322-334.
3. Geffe, P.R., An Open Letter to Communication Engineers, Proceedings IEEE, Vol. 55, 1967, p. 2173.
4. Gill, A., Linear Sequential Circuits, McGraw-Hill, 1966.
5. Gitlin, R.D. et al., Timing Recovery and Scramblers in Data Transmission, The B.S.T.J., March 1975, pp. 569-593.
6. Henrikson, U., On a Scrambling Property of Feedback Shift Registers, IEEE Transactions on Communications, Vol. COM-20, No. 5, October 1972, pp. 998-1001.
7. Kasai, H. et al., PCM Jitter Supression by Scrambling, IEEE Transactions on Communications, Vol. COM-22, August 1974, pp. 1114-1122.
8. Leeper, D.G., A Universal Digital Data Scrambler, The B.S.T.J., December 1973, pp. 1851-1865.
9. MacWilliams, F.J. and Sloane, N.J.A., Psedu Random Sequences and Arrays, IEEE Proceedings, December 1976, pp. 1715-1728.
10. Nakamura, K. et al., Data Scramblers for Multilever Pulse Sequences, Electronics and Communications in Japan, Vol. 55-A, No. 6, 1972, p. 18.-16.
11. Petrovic, G., Spectrum of Scrambled Signal, Electronic Letters, Vol. 16, No. 4, 14 February 1980, pp. 147-148.
12. Sam Shanmugam, K., Digital and Analog Communication Systems, John-Wiley, 1979, pp. 240-242 and 405.
13. Sangani, S., A Spectral Theoretic Approach to Fault Analysis in Linear Sequential Circuits, Texas Tech. University, August 1975, pp. 18-24.
14. Savage, J.E., Some Simple Self-Synchronising Digital Data Scramblers, The B.S.T.J., February 1967, pp. 449-487.

15. Yarlagadda, R., Benchmark Synchronisation of M-sequences, Electronic Letters, 21 January 1982, Vol. 18, No. 2, pp. 68-69.
16. Transmission Systems for Communications, Bell Telephone Laboratory, 4th Edition, February 1970, pp. 132, 657 and 658.

## APPENDIX A

OPERATION TABLES FOR GF(2<sup>2</sup>), GF(2<sup>3</sup>), GF(2<sup>4</sup>) AND GF(2<sup>5</sup>)

This appendix presents the operation tables for the Galois fields GF(2<sup>n</sup>), for n = 2, 3, 4 and 5. The irreducible polynomial used to generate these fields is also indicated.

1. GF(2<sup>2</sup>); (0, 1, a, a<sup>2</sup>): g(x) = x<sup>2</sup> + x + 1

Table A.1 Addition Table for GF(2<sup>2</sup>)

+	0	1	a	a <sup>2</sup>
0	0	1	a	a <sup>2</sup>
1	1	0	a <sup>2</sup>	a
a	a	a <sup>2</sup>	0	1
a <sup>2</sup>	a <sup>2</sup>	a	1	0

Multiplication: a<sup>i</sup> . a<sup>j</sup> = a<sup>(i+j) mod 3</sup>

2. GF(2<sup>3</sup>); (0, 1, a, a<sup>2</sup>, ..., a<sup>6</sup>); g(x) = x<sup>3</sup> + x + 1

Table A.2. Addition Table for  $GF(2^3)$ 

+	0	1	a	$a^2$	$a^3$	$a^4$	$a^5$	$a^6$
0	0	1	a	$a^2$	$a^3$	$a^4$	$a^5$	$a^6$
1	1	0	$a^3$	$a^6$	a	$a^5$	$a^4$	$a^2$
a	a	$a^3$	0	$a^4$	1	$a^2$	$a^6$	$a^5$
$a^2$	$a^2$	$a^6$	$a^4$	0	$a^5$	a	$a^3$	1
$a^3$	$a^3$	a	1	$a^5$	0	$a^6$	$a^2$	$a^4$
$a^4$	$a^4$	$a^5$	$a^2$	a	$a^6$	0	1	$a^3$
$a^5$	$a^5$	$a^4$	$a^6$	$a^3$	$a^2$	1	0	a
$a^6$	$a^6$	$a^2$	$a^5$	1	$a^4$	$a^3$	a	0

Multiplication:  $a^i \cdot a^j = a^{(i+j) \bmod 7}$

3.  $GF(2^4)$ ;  $(0, 1, a, a^2, \dots, a^{14})$ ,  $g(x) = a^4 + x + 1$

Table A.3\* Addition Table for  $GF(2^4)$

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	5	9	15	2	11	14	10	3	8	6	13	12	7	4
2	2	5	0	6	10	1	3	12	15	11	4	9	7	14	13	8
3	3	9	6	0	7	11	2	4	13	1	12	5	10	8	15	14
4	4	15	10	7	0	8	12	3	5	14	2	13	6	11	9	1
5	5	2	1	11	8	0	9	13	4	6	15	3	14	7	12	10
6	6	11	3	2	12	9	0	10	14	5	7	1	4	15	8	13
7	7	14	12	4	3	13	10	0	11	15	6	8	2	5	1	9
8	8	10	15	13	5	4	14	11	0	12	1	7	9	3	6	2
9	9	3	11	1	14	6	5	15	12	0	13	2	8	10	4	7
10	10	8	4	12	2	15	7	6	1	13	0	14	3	9	11	5
11	11	6	9	5	13	3	1	8	7	2	14	0	15	4	10	12
12	12	13	7	10	6	14	4	2	9	8	3	15	0	1	5	11
13	13	12	14	8	11	7	15	5	3	10	9	4	1	0	2	6
14	14	7	13	15	9	12	8	1	6	4	11	10	5	2	0	3
15	15	4	8	14	1	10	13	9	2	7	5	12	11	6	3	0

\*Mapping of elements is:  $0 \rightarrow 0$  and  $i + 1 \rightarrow a^i$ ,

$i = 0, 1, \dots, 14$

Table A.4 Addition table for  $GF(2^5)$ 

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	19	6	30	11	3	28	23	21	17	5	20	24	15	14	25	10	31	2	12	9	26	8	13	16	22	29	7	27	4	18
2	19	0	20	7	31	12	4	29	24	22	18	6	21	25	16	15	28	11	1	3	13	10	27	9	14	17	23	30	8	28	5
3	5	20	0	21	8	1	13	5	30	25	23	19	7	22	26	17	16	27	12	2	4	14	11	28	10	15	18	24	31	9	29
4	30	7	21	0	22	9	2	14	6	31	26	24	20	8	23	27	18	17	28	13	3	5	15	12	29	11	16	19	25	1	10
5	11	31	8	22	0	23	10	3	15	7	1	27	25	21	9	24	28	19	18	29	14	4	6	16	13	30	12	17	20	26	2
6	3	12	1	9	23	0	24	11	4	16	8	2	28	26	22	10	25	29	20	19	30	15	5	7	17	14	31	13	18	21	27
7	28	4	13	2	10	24	0	25	12	5	17	9	3	29	27	23	11	26	30	21	20	31	15	6	8	18	15	1	14	19	22
8	23	29	5	14	3	11	25	0	26	13	6	18	10	4	30	28	24	12	27	31	22	21	1	17	7	9	19	16	2	15	20
9	21	24	30	6	15	4	12	26	0	27	14	7	19	11	5	31	29	25	13	28	1	23	22	2	18	8	10	20	17	3	16
10	17	22	25	31	7	16	5	13	27	0	28	15	8	20	12	6	1	30	25	14	29	2	24	23	3	19	9	11	21	18	4
11	5	18	23	26	1	8	17	6	14	28	0	29	16	9	21	13	7	2	31	27	15	30	3	25	24	4	21	10	12	22	19
12	20	6	19	24	27	2	9	18	7	15	29	0	30	17	10	22	14	8	3	1	28	16	31	4	26	25	5	21	11	13	23
13	24	21	7	20	25	28	3	10	19	8	16	30	0	31	18	11	23	15	9	4	2	29	17	1	5	27	25	6	22	12	14
14	15	25	22	8	21	26	29	4	11	20	9	17	31	0	1	19	14	24	16	10	5	3	30	19	2	6	28	27	7	23	13
15	14	16	26	23	9	22	27	30	5	12	21	10	18	1	0	2	20	13	25	17	11	6	4	31	19	3	7	29	28	8	24
16	25	15	17	27	24	10	23	28	31	6	13	22	11	19	2	0	3	21	14	26	18	12	7	5	1	20	4	8	30	29	9
17	10	26	16	18	28	25	11	24	29	1	7	14	23	12	20	3	0	4	22	15	27	19	13	8	6	2	21	5	9	31	30
18	31	11	27	17	19	29	26	12	25	30	2	9	15	24	13	21	4	0	5	23	16	28	20	14	9	7	3	22	6	10	1
19	2	1	12	28	18	20	30	27	13	26	31	3	9	16	25	14	22	5	0	6	24	17	29	21	15	10	8	4	23	7	11
20	12	3	2	13	29	19	21	31	28	14	27	1	4	10	17	26	15	23	6	0	7	25	18	30	22	15	11	9	5	24	3
21	9	13	4	3	14	30	20	22	1	29	15	28	2	5	11	18	27	16	24	7	0	8	26	19	31	23	17	12	10	6	25
22	26	10	14	5	4	15	31	21	23	2	30	16	29	3	6	12	19	28	17	25	8	0	9	27	20	1	24	18	13	11	7
23	8	27	11	15	6	5	16	1	22	24	3	31	17	30	4	7	13	20	29	18	26	9	0	10	28	21	2	25	19	14	12
24	13	9	28	12	16	7	5	17	2	23	25	4	1	18	31	5	8	14	21	30	19	27	10	0	11	29	22	3	26	20	15
25	16	14	10	29	13	17	8	7	18	3	24	26	5	2	19	1	6	9	15	22	31	20	28	11	0	12	30	23	4	27	21
26	22	17	15	11	30	14	18	9	8	19	4	25	27	6	3	20	2	7	10	16	23	1	21	29	12	0	13	31	24	5	28
27	29	23	18	16	12	31	15	19	10	9	20	5	26	28	7	4	21	3	9	11	17	24	2	22	30	13	0	14	1	25	6
28	7	30	24	19	17	13	1	16	20	11	10	21	6	27	29	8	5	22	4	9	12	18	25	3	23	31	14	0	15	2	26
29	27	8	31	25	20	18	14	2	17	21	12	11	22	7	28	30	9	6	23	5	10	13	19	26	4	24	1	18	0	16	3
30	4	28	9	1	26	21	19	15	3	18	22	13	12	23	8	29	31	10	7	24	6	11	14	20	27	5	25	2	16	0	17
31	18	5	29	10	2	27	22	20	16	4	19	23	14	13	24	9	30	1	11	8	25	7	12	15	21	28	5	25	3	17	0

Mapping of field elements: 0 to 0 and  $i+1$  to  $a^i$ ,  $i=0, 1, \dots, 30$

Multiplication:  $a \cdot a = a^2$

## APPENDIX B

EIGENVALUES AND SPECTRAL COEFFICIENTS FOR VARIOUS STAGES OF SCRAMBLERS

Note: Wherever \* is put as superscript to table numbers;  
 mapping of elements of  $GF(2^n)$  is as follows:

$$0 \rightarrow 0,$$

$$i + 1 \rightarrow a^i, \quad i = 0, 1, \dots, 2^n - 2.$$

Table B.1 Eigenvalues and Unique States in  $GF(2^3)$ ;  
 $c(x) = x^3 + x^2 + 1$

e	$x_e$			$s(e)$
	$x_1$	$x_2$	$x_3$	
1	1	1	1	1
$a$	$a^5$	$a^4$	$a^3$	$a^6$
$a^2$	$a^3$	$a$	$a^6$	$a^6$
$a^4$	$a^6$	$a^2$	$a^5$	$a^3$

Table B.2\* Spectral Coefficients and Input at Output for Sequence of Period 7;  $c(x) = x^3 + x^2 + 1$

Critical States $x_c$	Input/Output Sequences	Input/Output Spectral Coefficients						
000	1111111,...	1	0	0	0	0	0	0
	1011000,...	1	0	0	3	0	2	5
000	1110100,...	0	0	0	1	0	1	1
	1010100,...	1	7	6	6	4	7	4
000	0111010,...	0	0	0	5	0	3	2
	0101010,...	1	6	4	3	7	2	5
000	0011101,...	0	0	0	2	0	5	3
	0010101,...	1	5	2	7	3	4	6
001	0011101,...	0	0	0	0	0	0	0
	1110100,...	0	0	0	1	0	1	1

Table B.3\* Eigenvalues and Unique States in  $GF(2^4)$ ;  
 $c(x) = x^3 + x^2 + 1$

e	$x_1$	$x_e$ $x_2$	$x_3$	$s(e)$
1	1	1	1	1
2	5	4	3	6
3	9	7	5	11
4	12	9	6	15
5	2	13	9	6
6	1	11	6	6
7	8	2	11	14
8	13	6	14	5
9	3	10	2	11
10	14	5	11	8
11	1	6	11	11
12	7	11	15	3
13	15	3	6	12
14	4	6	8	2
15	10	11	12	9

Table 8.4 Spectral coefficients at input and output for sequences of period 15:  $c(x) = x^3 + x^2 + 1$

Critical States	Input/Output Spectral coefficients														
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
111	1	5	11	15	6	6	14	6	11	8	11	3	12	2	9
110	2	15	14	13	12	11	10	9	8	7	6	5	4	3	2
100	1	14	12	10	8	6	4	2	15	13	11	9	7	5	3
001	1	13	10	7	4	1	13	10	7	4	1	13	10	7	4
010	1	12	8	4	15	11	7	3	14	10	6	2	13	9	5
101	1	11	6	1	11	6	1	11	6	1	6	11	8	12	14
011	1	10	4	13	7	1	10	4	13	7	1	10	4	13	7
111	1	9	2	10	3	11	4	12	5	13	6	14	7	15	8
110	1	14	12	9	8	1	2	1	15	5	1	1	3	1	1
100	1	8	15	7	14	6	13	5	12	4	11	3	10	2	9
001	1	13	10	6	4	11	11	9	7	11	6	5	6	3	2
100	1	7	13	4	10	1	7	13	4	10	1	7	13	4	10
001	1	12	8	3	15	6	5	2	14	2	11	9	5	3	2
010	1	6	11	1	6	11	1	14	10	6	11	1	11	7	14
101	1	11	6	15	11	1	14	10	6	11	1	11	12	7	4
011	1	5	9	13	2	6	10	14	3	13	7	11	15	4	9
111	1	10	4	12	7	11	8	3	13	14	5	11	2	15	5
101	1	9	2	10	13	1	6	2	11	5	5	11	4	7	13
011	1	3	5	7	9	11	12	15	2	4	6	8	10	12	14
111	1	8	15	6	14	4	11	4	12	11	1	10	6	13	7
110	1	7	13	3	10	11	5	12	4	10	11	6	14	9	15

Table 8.5\* Eigenvalues and Unique States in  $GF(2^5)$ :  
 $c(x) = x^3 + x^2 + 1$

e	X(e)			S(e)
	$x_1$	$x_2$	$x_3$	
1	1	1	1	1
2	26	25	24	27
3	20	18	16	22
4	28	25	22	31
5	8	4	31	12
6	19	14	9	24
7	24	18	12	30
8	13	6	30	20
9	15	7	30	23
10	21	12	3	30
11	6	27	17	15
12	19	8	28	30
13	16	4	23	23
14	11	29	16	21
15	25	11	28	8
16	19	4	20	3
17	29	13	27	14
18	30	13	27	15
19	10	23	5	29
20	7	19	31	25
21	11	22	2	31
22	10	20	30	31
23	6	15	24	28
24	10	18	26	2
25	31	7	14	24
26	4	10	16	29
27	21	26	31	16
28	21	25	29	17
29	18	21	24	15
30	11	13	15	9
31	6	7	8	5

Table 8.6 Spectral Coefficients at Input and Output for Sequences of Period 31;  $c(x) = x^3 + x + 1$

S1	critical No	State	Input/Output Spectral Coefficients																																				
			1	0	0	1	1	1	1	27	22	31	12	24	30	20	1	23	30	16	30	28	24	18	13	14	16	28	26	31	31	28	1	2	24	1	29	16	17
1	0	0	1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	6	5			
2	0	0	1	1	26	20	28	8	19	24	13	15	21	6	19	16	11	25	19	29	30	10	7	11	10	6	10	31	4	21	21	18	11	6					
3	0	1	0	1	30	28	26	24	22	20	19	16	14	12	10	8	6	4	2	31	29	27	25	23	21	19	17	15	13	11	9	7	5	3	2				
4	1	0	1	1	29	26	23	20	17	14	11	8	5	2	30	27	24	21	18	15	12	9	6	3	31	28	25	22	19	16	13	10	7	4					
5	0	1	1	1	1	28	24	20	16	12	8	4	31	27	23	19	15	11	7	3	30	26	22	18	14	10	6	2	29	25	21	17	13	9	5				
6	1	1	1	1	1	27	22	17	12	7	2	28	23	18	13	8	3	29	24	19	14	9	4	30	25	20	15	10	5	31	26	21	16	11	6				
7	1	1	0	1	1	26	20	14	8	2	27	21	15	9	3	28	22	16	10	4	29	23	17	11	5	30	24	18	12	6	31	25	19	13	7				
8	1	0	0	1	1	25	18	11	4	28	21	14	7	31	24	17	10	3	27	20	13	6	30	23	16	9	2	26	19	12	5	29	22	15	3				
9	0	0	1	1	1	24	16	8	31	23	15	7	30	22	14	6	29	21	13	5	28	20	12	4	27	19	11	3	26	18	10	2	25	17	9				
10	0	1	0	1	1	23	14	5	27	18	9	31	22	13	4	26	17	8	30	21	12	3	25	16	7	29	20	11	2	24	15	6	28	19	10				
11	1	0	1	1	1	22	12	2	23	13	3	24	14	4	25	15	5	26	16	6	27	17	7	28	18	8	29	19	9	30	20	10	31	21	11				
12	0	1	1	1	1	21	10	30	19	8	28	17	6	26	15	4	24	13	2	22	11	31	20	9	29	18	7	27	16	5	25	14	3	23	12				
13	1	1	1	1	1	20	8	27	15	3	22	10	29	17	5	24	12	31	19	7	26	14	2	21	9	28	16	4	23	11	30	18	0	25	13				
14	1	1	0	1	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14				
15	1	0	0	1	1	18	4	21	7	24	10	27	13	30	16	2	19	5	22	8	25	11	28	14	31	17	3	20	5	23	9	26	12	20	15				
16	0	0	1	1	17	2	18	3	19	4	20	5	21	6	22	7	23	8	24	9	25	10	26	11	27	12	28	13	29	14	30	15	31	16					
17	0	1	0	1	1	16	31	15	30	14	29	13	28	12	27	11	26	10	25	9	24	8	23	7	22	6	21	5	20	4	19	3	18	2	17				
18	1	0	1	1	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	16	30	13	27	10	24	7	21	4	18				
19	0	1	1	1	1	14	27	9	22	4	17	30	12	25	7	20	2	15	28	10	23	5	18	31	13	26	8	21	3	15	29	11	24	6	19				
20	1	1	1	1	1	13	25	6	18	30	11	23	4	16	28	9	21	2	14	26	7	19	31	12	24	5	17	29	10	22	3	15	27	8	20				
21	1	1	0	1	1	12	23	3	14	25	5	16	27	7	18	29	9	20	31	11	22	2	13	24	4	15	26	6	17	28	8	19	30	10	21				

(contd.)

(Table 8.6 contd)

Sl No	critical State	Input/Output Spectral Coefficients																																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36					
22	1 0 0	1	11	21	31	10	20	30	9	19	29	8	18	28	7	17	27	6	16	26	5	15	25	4	14	24	3	13	23	2	12	22	9	16	20	26						
23	0 0 1	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22	31	9	18	27	5	14	23	6	2	12	19	22	27				
24	0 1 0	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23	31	8	16	24	1	16	22	24	28					
25	1 0 1	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24	31	7	14	21	28	4	11	19	25	1	18	20	25	26	29				
26	0 1 1	1	7	13	19	25	31	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	26	30	3	24	17	24	28	30			
27	1 1 1	1	6	11	16	21	26	31	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27	1	30	22	28	31	30	31			
28	1 1 0	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27	31	4	8	12	16	20	24	28	1	27	5	27	1	3	1			
29	1 0 0	1	4	7	10	13	16	19	22	25	28	31	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	26	29	1	1	9	3	11	1	5	6	3	2
30	0 0 1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	6	9	9	5	3	3				
31	0 1 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	7	4	1	1	1	1				

Table B.7\* Eigenvalues and Unique States in  $GF(2^5)$   
 $C(x)=x^4+x+1$

e	x(e)				s(e)
	$x_1$	$x_2$	$x_3$	$x_4$	
1	1	1	1	1	1
2	18	17	16	15	19
3	4	2	31	29	6
4	30	27	24	21	2
5	7	3	30	26	11
6	13	8	3	29	19
7	28	22	16	10	3
8	4	28	21	14	11
9	13	5	28	20	21
10	1	26	17	8	13
11	25	15	5	26	4
12	25	14	3	22	5
13	24	12	31	19	5
14	4	22	9	27	17
15	7	24	10	27	21
16	20	5	21	6	4
17	25	9	24	8	10
18	31	14	28	11	17
19	7	20	2	15	25
20	18	30	11	23	6
21	18	29	9	20	7
22	13	23	2	12	3
23	18	27	5	14	9
24	26	3	11	19	18
25	16	23	30	6	9
26	25	31	6	12	19
27	7	12	17	22	2
28	29	2	6	10	25
29	13	16	19	22	10
30	15	17	19	21	13
31	8	9	10	11	7

Table B.8 Spectral Coefficients at Input and Output for Sequences of Period 31;  $c(x) = x^4 + x + 1$

(Table b.8 contd)

S1	critical	Input/Output Spectral Coefficients																																	
No	State																																		
22	0110	1	11	21	31	10	20	30	9	19	29	8	18	28	7	17	27	6	16	26	5	15	25	4	14	24	3	13	23	212	22				
		1	29	26	1	20	6	1	19	8	10	11	22	1	23	6	30	15	1	19	10	21	27	12	31	1	21	14	16	11	24	28			
23	1100	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22	31	9	18	27	5	14	23			
		1	28	24	29	16	1	26	12	31	1	11	20	10	23	15	30	15	1	22	1	6	21	8	8	27	19	20	14	26	29				
24	1001	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23	31	8	16	29			
		1	27	22	25	12	27	20	5	23	23	22	31	8	28	9	31	14	29	14	3	12	16	30	16	15	32	24	24	17	28	30			
25	0010	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24	31	7	14	21	28	4	11	18	25	30	31	
		1	26	20	23	8	22	14	29	15	14	12	20	27	15	26	16	29	12	27	15	23	26	8	24	22	8	29	28	20	30	31			
26	0100	1	7	13	19	25	31	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	26	1		
		1	25	18	20	4	17	8	22	7	5	2	9	15	2	12	1	13	26	9	27	3	5	17	1	29	14	3	1	23	1	1			
27	1000	1	6	11	16	21	26	31	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27			
		1	24	16	17	31	12	2	15	30	27	23	29	3	20	29	17	28	9	22	8	14	15	26	9	5	20	8	5	26	3	2			
28	0001	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27	31	4	8	12	15	20	24	28	5	3	
		1	23	14	14	27	7	27	8	22	18	13	18	22	7	15	2	12	23	4	20	25	25	4	17	12	12	26	13	9	29	5	3		
29	0011	1	4	7	10	13	16	19	22	25	28	31	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	25	29	7		
		1	22	12	11	23	2	21	1	14	9	3	7	10	25	1	18	27	6	17	1	5	4	13	25	19	1	18	13	1	7	4			
30	0111	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	4	9	5
		1	21	10	8	19	28	15	25	6	31	24	27	29	12	18	3	11	20	30	13	16	14	22	2	26	7	23	17	8	9	5			
31	1111	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	7	11	6

For serial number  $i$ , the input sequence is  $D^{i-1}u(t)$  and the output sequence is  $D^{i-1}v(t)$ ; where  $u(t)$  is  $10000000000000000000000000000000,10\ldots$  and  $v(t)$  is  $100010011010111000100110101111,10\ldots$

Table B.9 Eigenvalue and Unique States in  $GF(2^4)$ ;  
 $c(x)=x^4 + x^3 + x + 1$

e	x(e)				s(e)
	$x_1$	$x_2$	$x_3$	$x_4$	
1	1	1	1	1	1
2	3	2	1	3	1
3	2	3	1	2	1

Table B.10 Spectral coefficients at Input and Output  
 $c(x)=x^4 + x^3 + x + 1$

Critical states	Input/Output Sequences			Input/Output Spectral Coefficients		
0 0 1 0	1	0	0	1	1	1
	1	0	0	1	1	1
0 1 0 0	0	1	0	1	3	2
	0	1	0	1	3	2
1 0 0 1	0	0	1	1	2	3
	0	0	1	1	2	3

\*  
Table B.11 Eigenvalues and Unique States in  $GF(2^3)$ ;  
 $c(x)=x^4 + x^3 + 1$

e	X(e)				S(e)
	X <sub>1</sub>	X <sub>2</sub>	X <sub>3</sub>	X <sub>4</sub>	
1	1	1	1	1	1
2	2	1	7	6	3
3	3	1	6	4	5
4	2	6	3	7	5
5	5	1	4	7	2
6	5	7	2	4	3
7	3	4	5	6	2

\*  
Table B.12 Spectral Coefficients at Input and Output  
 $c(x)=x^4 + x^3 + 1$

Critical states	Input/Output Sequences	Input/Output spectral coefficients						
		1	1	1	1	1	1	1
1 1 0 1	1 0 0 0 0 0 0	1	1	1	1	1	1	1
	1 1 0 1 0 1 1	1	3	5	5	2	3	2
1 0 1 0	0 1 0 0 0 0 0	1	7	6	5	4	3	2
	1 1 1 0 1 0 1	1	2	3	2	5	5	3
0 1 0 1	0 0 1 0 0 0 0	1	6	4	2	7	5	3
	1 1 1 1 0 1 0	1	1	1	6	1	7	4
1 0 1 1	0 0 0 1 0 0 0	1	5	2	6	3	7	4
	0 1 1 1 1 0 1	1	7	6	3	4	2	5
0 1 1 1	0 0 0 0 1 0 0	1	4	7	3	6	2	5
	1 0 1 1 1 1 0	1	6	4	7	7	4	6
1 1 1 1	0 0 0 0 0 1 0	1	3	5	7	2	4	6
	0 1 0 1 1 1 1	1	5	2	4	3	6	7
1 1 1 0	0 0 0 0 0 0 1	1	2	3	4	5	6	7
	1 0 1 0 1 1 1	1	4	7	1	6	1	1

Table 8.13 Eigenvalues and Unique States in  $GF(2^4)$ 

$$c(x) = x^4 + x^3 + 1$$

e	X(e)				S(e)
	X <sub>1</sub>	X <sub>2</sub>	X <sub>3</sub>	X <sub>4</sub>	
1	1	1	1	1	1
2	10	9	8	7	11
3	4	2	15	13	6
4	8	5	2	14	11
5	7	3	14	10	11
6	11	6	1	11	1
7	15	9	3	12	6
9	13	5	12	4	6
10	12	3	9	15	6
11	6	11	1	6	1
13	14	2	5	8	11

Eigenvalues are not defined for e=9, 12, 14 and 15.

Table 8.14 Spectral Coefficients at Input and Output

$$for Sequences of Period 5; c(x) = x^4 + x^3 + 1$$

Critical States	Input/Output	Spectral Coefficients
0110	1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0	1 0 0 11 0 0 5 0 0 6 0 0 11 0 0 0
1101	1 0 0 13 0 0 0 10 0 0 0 7 0 0 0 4 0 0	1 0 0 8 0 0 15 0 0 12 0 0 14 0 0 0 0 0
1010	1 0 0 10 0 0 0 4 0 0 0 13 0 0 0 7 0 0 0	1 0 0 5 0 0 9 0 0 3 0 0 13 0 0 2 0 0 0
0101	1 0 0 7 0 0 0 13 0 0 0 4 0 0 0 10 0 0 0	1 0 0 2 0 0 3 0 0 0 0 0 5 0 0 0 0 0 0 0
1011	1 0 0 4 0 0 0 7 0 0 0 10 0 0 0 13 0 0 0 0	1 0 0 14 0 0 12 0 0 15 0 0 13 0 0 8 0 0 0 0

Table 8.15 Spectral Coefficients at Input and Output  
for Sequences of Period 15 if  $f(x) = x^4 + x^3 + 1$

Si. No.	Critical States	Input/Output	Spectral Coefficients
1.	0000	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 0 0 0 0 0 0 6 0 0 0 0 11 0 6 11
2/1	0000	0 0 0 0 0 0 5 0 0 3 0 0 11 2 0 0 9 5	0 0 0 0 0 0 5 0 0 3 0 0 11 2 0 0 9 5
2/2	0000	0 0 0 0 0 1 0 0 0 0 0 1 6 0 0 11 6	0 0 0 0 0 1 0 0 0 0 0 1 6 0 0 11 6
3/1	0000	0 0 0 12 0 0 0 13 0 5 0 0 14 0 0 3 10 2 0	0 0 0 12 0 0 0 13 0 5 0 0 14 0 0 3 10 2 0
3/2	0000	0 0 0 9 0 0 0 2 0 13 0 0 10 0 0 7 13 3 0 10	0 0 0 9 0 0 0 2 0 13 0 0 10 0 0 7 13 3 0 10
3/3	0000	0 0 0 6 0 0 0 11 0 1 0 0 11 0 0 11 1 6 0 11	0 0 0 6 0 0 0 11 0 1 0 0 11 0 0 11 1 6 0 11
3/4	0000	0 0 0 3 0 0 0 5 0 0 14 0 0 2 0 0 15 4 0 12	0 0 0 3 0 0 0 5 0 0 14 0 0 2 0 0 15 4 0 12
4/1	0000	0 4 7 0 13 0 0 0 11 0 10 0 0 0 0 6 0 0 3 0	0 4 7 0 13 0 0 0 11 0 10 0 0 0 0 6 0 0 3 0
4/2	0000	0 3 5 0 9 0 0 0 4 0 2 0 0 0 10 0 0 0 13 0	0 3 5 0 9 0 0 0 4 0 2 0 0 0 10 0 0 0 13 0
4/3	0000	0 2 3 0 5 0 0 0 12 0 9 0 0 0 14 0 0 0 15 0	0 2 3 0 5 0 0 0 12 0 9 0 0 0 14 0 0 0 15 0
4/4	0000	0 1 1 0 1 0 0 0 5 0 6 0 0 0 3 0 0 2 0	0 1 1 0 1 0 0 0 5 0 6 0 0 0 3 0 0 2 0
5	0001	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

Input for serial no 1 is 1111111111111111...

Input for serial no 1/1 is  $0^{1*1} u(i,t)$ ,  $i=2,3,4$  and  $i=1,2,3,4$

$u(2,t)$  is 1101101101101101...

$u(3,t)$  is 11000110001100001...

$u(4,t)$  is 10011010111100001...

The last column gives spectral coefficients of the zero input response for the state 0 0 0 1.

The output sequence for serial no 1 is 101001101110001...

Output for serial no 1/1 is  $0^{1*1} v(i,t)$ ,  $i=2,3,4$  and  $i=1,2,3,4$

$v(2,t)$  is 10011100110000001...

$v(3,t)$  is 10001011000000001...

$v(4,t)$  is 11100111000000001...

Table B.16 Eigenvalues and Unique States in  $GF(2^5)$ ;  
 $C(x) = x^4 + x^3 + 1$

e	X(e)				S(e)
	$x_1$	$x_2$	$x_3$	$x_4$	
1	1	1	1	1	1
2	10	9	8	7	11
3	19	17	15	13	21
4	19	16	13	10	22
5	6	2	29	25	10
6	17	12	7	2	22
7	6	31	25	19	12
8	30	23	16	9	6
9	11	3	26	18	19
10	5	27	18	9	14
11	2	23	13	3	12
12	9	29	18	7	20
13	11	30	18	6	23
14	2	20	7	25	15
15	28	14	31	17	11
16	24	9	25	10	8
17	21	5	20	4	6
18	10	24	7	21	27
19	9	22	4	17	27
20	31	12	24	5	19
21	3	14	25	5	23
22	5	15	25	4	26
23	17	26	4	13	8
24	28	5	13	21	20
25	21	28	4	11	14
26	16	22	28	3	10
27	3	8	13	18	29
28	30	3	7	11	26
29	24	27	30	2	21
30	31	2	4	6	29
31	16	17	18	19	15

Table B.17 Spectral Coefficients at Input and Output for Sequences of Period 31;  $c(x) = x^4 + x^3 + 1$

S <sub>1</sub>	critical	Input/Output Spectral Coefficients																																				
No	State	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
1	1111	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
2	1110	1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2						
3	1100	1	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2	31	29	27	25	23	21	19	17	15	13	11	9	7	5	3	2					
4	1000	1	29	26	23	20	17	14	11	8	5	2	30	27	24	21	18	15	12	9	6	3	31	28	25	22	19	16	13	10	7	4						
5	0001	1	28	24	20	16	12	8	4	31	27	23	19	15	11	7	3	30	26	22	18	14	10	6	2	29	25	21	17	13	9	5	2	6	19			
6	0010	1	27	22	17	12	7	2	28	23	18	13	8	3	29	24	19	14	9	4	30	25	20	15	10	5	31	26	21	16	11	6	8	20				
7	0100	1	26	20	14	8	2	27	21	15	9	3	28	22	16	10	4	29	23	17	11	5	30	24	18	12	6	31	25	19	13	7	10	21				
8	1001	1	25	18	11	4	28	21	14	7	31	24	17	10	3	27	20	13	6	30	23	16	9	2	26	19	12	5	29	22	15	8	11	12	22			
9	0011	1	24	16	8	31	23	15	7	30	22	14	6	29	21	13	5	28	20	12	4	27	19	11	3	26	18	10	2	25	17	9	14	14	23			
10	0110	1	23	14	5	27	18	9	31	22	13	4	26	17	8	30	21	12	3	25	16	7	29	20	11	2	24	15	6	28	19	10	2	12	31	17	16	24
11	1101	1	22	12	2	23	13	3	24	14	4	25	15	5	26	16	6	27	17	7	28	18	8	29	19	9	30	20	10	31	21	11	4	20	18	25		
12	1010	1	21	10	30	19	8	28	17	6	26	15	4	24	13	2	22	11	31	20	9	29	18	7	27	16	5	25	14	3	23	12	8	23	20	26		
13	0101	1	20	8	27	15	3	22	10	29	17	5	24	12	31	19	7	26	14	2	21	9	28	15	4	23	11	30	18	6	25	13	27	12	26	22	27	
14	1011	1	19	6	24	11	29	16	3	21	8	26	13	31	18	5	23	10	28	15	2	20	7	25	12	30	17	4	22	9	27	14	1	15	29	24	26	
15	0111	1	18	4	21	7	24	10	27	13	30	16	2	19	5	22	8	25	11	28	14	31	17	3	20	6	23	11	10	8	19	1	6	20	1	26	29	
16	1111	1	17	2	18	3	19	4	20	5	21	6	22	7	23	8	24	9	25	10	26	11	27	12	28	13	29	14	30	15	31	10	4	28	30			
17	1110	1	16	31	15	30	14	29	13	28	12	27	11	26	10	25	9	24	8	23	7	22	6	21	5	20	4	19	3	18	2	17	7	30	31			
18	1100	1	15	29	12	26	9	23	6	20	3	17	31	14	28	11	25	8	22	5	19	2	13	17	31	10	7	21	8	18	1	1	1	1	1			
19	1000	1	14	27	9	22	4	17	30	12	25	7	20	2	15	28	10	23	5	18	31	13	26	8	21	3	16	29	11	24	6	19						
20	0001	1	13	25	6	18	30	11	23	4	16	28	9	21	2	14	26	7	19	31	12	24	5	17	29	10	22	3	15	27	8	20	5	3				
21	0010	1	12	23	3	14	25	5	16	27	7	18	29	9	20	31	11	22	2	13	24	4	15	26	6	17	28	8	19	30	10	21	7	4				

(contd.)

(Table 8.17 contd)

S1	critical	Input/Output Spectral Coefficients																																	
No	State	1	11	21	31	10	20	30	9	19	29	8	18	28	7	17	27	2	16	26	5	15	25	4	14	24	3	13	23	2	12	22	9	5	
22	0100	1	11	21	31	10	20	30	9	19	29	8	18	28	7	17	27	2	16	26	5	15	25	4	14	24	3	13	23	2	12	22	9	5	
23	1001	1	10	19	28	6	15	24	2	11	20	29	7	16	25	3	12	21	30	8	17	26	4	13	22	31	9	18	27	5	14	23	11	6	
24	0011	1	9	17	25	2	10	18	26	3	11	19	27	4	12	20	28	5	13	21	29	6	14	22	30	7	15	23	31	8	16	24	13	7	
25	0110	1	8	15	22	29	5	12	19	26	2	9	16	23	30	6	13	20	27	3	10	17	24	31	7	14	21	28	4	11	18	25	31	15	8
26	1101	1	7	13	19	25	31	6	12	18	24	30	5	11	17	23	29	4	10	16	22	28	3	9	15	21	27	2	8	14	20	26	3	17	9
27	1010	1	6	11	16	21	26	31	5	10	15	20	25	30	4	9	14	19	24	29	3	8	13	18	23	28	2	7	12	17	22	27	6	19	10
28	0101	1	5	9	13	17	21	25	29	2	6	10	14	18	22	26	30	3	7	11	15	19	23	27	31	4	8	12	16	20	24	28	9	21	11
29	1011	1	4	7	10	13	16	19	22	25	28	31	3	6	9	12	15	18	21	24	27	30	2	5	8	11	14	17	20	23	26	29	12		
30	0111	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	13		
31	1111	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	14		

For serial number  $i$ , the input sequence is  $0^{\frac{i-1}{2}} u(t)$  and the output sequence is  $0^{\frac{i-1}{2}} y(t)$ ; where,  
 $u(t)$  is  $10000000000000000000000000000000, 10, \dots$  and  
 $y(t)$  is  $1010110010001111010110010001111, 10, \dots$

\* Table B.18 Eigenvalues and Unique States in  $GF(2^3)$ ;  
 $c(x)=x^5 + x^4 + x^2 + x + 1$

e	X(e)					S(e)
	$x_1$	$x_2$	$x_3$	$x_4$	$x_5$	
1	1	1	1	1	1	1
2	1	7	6	5	4	2
3	1	6	4	2	7	3
4	5	2	6	3	7	1
5	1	4	7	3	6	5
6	3	5	7	2	4	1
7	2	3	4	5	6	1

\* Table B.19 Spectral coefficients at Input and Output  
 $c(x)=x^5 + x^4 + x^2 + x + 1$

Critical States	Input/Output Sequences	Input/Output Spectral Coefficients
0 0 1 1 1	1 0 0 0 0 0 0	1 1 1 1 1 1 1
	0 0 1 1 1 0 0	1 2 3 1 5 1 1
0 1 1 1 0	0 1 0 0 0 0 0	1 7 6 5 4 3 2
	0 0 0 1 1 1 0	1 1 1 5 1 3 2
1 1 1 0 0	0 0 1 0 0 0 0	1 6 4 2 7 5 3
	0 0 0 0 1 1 1	1 7 6 2 4 5 3
1 1 0 0 0	0 0 0 1 0 0 0	1 5 2 6 3 7 4
	1 0 0 0 0 1 1	1 6 4 6 7 7 4
1 0 0 0 0	0 0 0 0 1 0 0	1 4 7 3 6 2 5
	1 1 0 0 0 0 1	1 5 2 3 3 2 5
0 0 0 0 1	0 0 0 0 0 1 0	1 3 5 7 2 4 6
	1 1 1 0 0 0 0	1 4 7 7 6 4 6
0 0 0 1 1	0 0 0 0 0 0 1	1 2 3 4 5 6 7
	0 1 1 1 0 0 0	1 3 5 4 2 6 7

\*  
 Table B.20 Eigenvalues and corresponding Unique States  
 In  $GF(2^4)$ ;  $c(x) = x^4 + x^5 + x^2 + x + 1$

e	X(e)					S(e)
	X <sub>1</sub>	X <sub>2</sub>	X <sub>3</sub>	X <sub>4</sub>	X <sub>5</sub>	
1	1	1	1	1	1	1
2	4	3	2	1	15	5
3	7	5	3	1	14	9
4	6	3	15	12	9	9
5	13	9	5	1	12	2
6	6	1	11	6	1	11
7	11	5	14	8	2	2
8	11	4	12	5	13	3
9	10	2	9	1	8	3
10	11	2	8	14	5	5
11	11	1	6	11	1	6
12	6	10	14	3	7	2
13	6	9	12	15	3	3
14	11	13	15	2	4	9
15	6	7	8	9	10	5

Table 8.21 Spectral Coefficients at Input and Output  
for Sequences of Period 15;  $c(x) = x^5 + x^4 + x^2 + 1$

Critical States	Input/Output	Spectral Coefficients
10011	1 5 9 9 2 11 1 2 3 3 5 6 1 2 3 9 1 5	1 1 5 9 9 2 11 1 2 3 3 5 6 1 2 3 9 1 5
00111	1 15 14 13 12 11 10 9 8 7 6 5 4 3 11 2	1 4 7 6 13 11 11 10 11 11 6 5 4 3 11 2
01110	1 14 12 10 8 6 4 2 15 13 12 11 9 7 5 3 7	1 3 5 3 9 1 5 4 2 15 13 12 11 9 7 5 3 7
11100	1 13 10 7 4 11 13 10 9 8 6 13 12 15 7 4	1 2 3 15 5 11 14 12 9 8 6 14 12 15 7 4
11000	1 12 8 4 15 11 6 7 3 14 10 6 2 13 9 5	1 1 12 8 12 1 6 7 3 14 10 6 2 13 9 5
10000	1 11 6 1 11 6 1 2 11 6 5 1 11 6 7 3 11 4 10	1 15 14 9 12 1 2 13 8 5 1 11 6 7 3 11 4 10
00001	1 10 4 13 7 1 10 4 13 7 1 10 4 13 6 5 11 7	1 14 12 6 8 11 11 6 15 11 6 11 4 13 6 5 11
00011	1 9 2 10 3 11 4 12 5 13 6 14 7 13 2 11 15 7 15 8	1 13 10 3 4 6 5 14 7 13 2 11 15 9 8 12
00110	1 8 15 7 14 6 13 5 12 4 11 3 10 2 10 1 13	1 12 8 15 15 1 14 7 14 8 11 3 12 10 1 13
01101	1 7 13 4 10 1 1 7 13 4 10 1 6 7 13 4 10	1 11 6 12 11 11 9 15 6 14 1 6 7 13 4 10
11010	1 6 11 1 6 11 2 6 11 5 11 6 11 12 3 14 6 11	1 10 4 9 7 6 5 11 2 8 13 5 11 12 3 14 6 11
10101	1 5 9 2 13 2 6 10 14 1 3 5 7 11 1 15 4 8 12	1 9 2 6 3 1 11 1 1 3 5 7 11 1 15 4 8 12
01010	1 4 7 10 13 1 4 7 10 13 1 6 4 7 10 3 2 6 5 9 10 13	1 8 15 3 14 11 5 9 12 13 2 6 5 9 10 3 2
10100	1 3 5 7 9 11 13 15 2 4 4 6 8 10 12 5 3	1 7 13 15 10 6 14 2 4 8 11 6 8 10 12 5 3
01001	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	1 6 11 12 1 6 1 7 8 10 11 14 1 13 15 7 14

\* Table B.22 Eigenvalues and Unique States in GF(2)<sup>5</sup>;

$$c(x) = x^5 + x^4 + x^2 + x + 1$$

e	X(e)					S(e)
	X <sub>1</sub>	X <sub>2</sub>	X <sub>3</sub>	X <sub>4</sub>	X <sub>5</sub>	
1	1	1	1	1	1	1
2	6	5	4	3	2	7
3	11	9	7	5	3	13
4	14	11	8	5	2	17
5	21	17	13	9	5	25
7	27	21	15	9	3	2
8	17	10	3	27	20	24
9	10	2	25	17	9	18
12	4	24	13	2	22	15
13	22	10	29	17	5	3
14	13	31	18	5	23	26
15	2	19	5	22	8	16
16	5	21	6	22	7	20
17	19	3	18	2	17	4
18	23	6	20	3	17	9
20	9	21	2	14	26	20
22	18	28	7	17	27	8
23	7	16	25	3	12	29
24	3	11	19	27	4	26
25	12	19	26	2	9	5
26	5	11	17	23	29	30
27	25	30	4	9	14	20
28	2	6	10	14	18	29
29	3	6	9	12	15	31
30	17	19	21	23	25	15
31	9	10	11	12	13	8

Note: Eigenvalues are not defined for e=6,10,11,19,21

Table B.23 Spectral Coefficients at Input and Output for Sequences of Period 31;  $c(x) = x^5 + x^4 + x^2$

(Contd.)

(Table 8.23 contd)

The last row gives spectral coefficients of the zero input response for the state 0 0 0 0 1

Input for serial no  $j/i$  is  $D^{i-1}u(j,t)$ ,  $j=2, \dots, 6$ , and  $i=1, 2, \dots, 5$ , where,

$$u(1,t)=1010111011000111110011010010000, \dots$$

$$u(2,t) = 110101001000101111011001110000, \dots$$

$$u(3,t)=110010011110111000101011010000, \dots$$

$$u(4,t)=1011010100011101111100100110000, \dots$$

$$u(5,t)=100101100111100011011101010000, \dots$$

Output for serial no 1 is 101110111010100

The zero input response for the state 0 0 0 0 1 is 11100110111

the zero input response for the state  $x(t)$  is

Output for serial no j/i is  $D^i y(j,t)$ ,  $j=2,3,\dots,6$ , and  $i=1,\dots,5$ , where,  
 $y(2,t)=11010101000101110100110000000000$

$$y(4, t) = 100110101001000011111110000000000, \dots$$

$$y(5, t) = 1100010101110101001101000000000, \dots$$